

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Охота на призраков: как понять, что инфраструктура не скомпрометирована

Софья Карева
менеджер продукта

Никита Гуцуляк
специалист по реагированию
на компьютерные инциденты

Перспективный мониторинг



ООО «Ромашка»

Ampire 360°



1 000 сотрудников

500 серверов

Есть небольшой ИБ -отдел

SOC работает 24/7

Есть определённая ИБ-инфраструктура.
Стоит SIEM, EDR, WAF, AV

Что бы мы сделали
в этой ситуации?



Недавно обнаружена подозрительная активность:
с произвольной периодичностью происходит
подключение с сервера к внешнему неизвестному
домену в рабочее время

Compromise Assessment ≠ пентест

Команда	Вопрос
Пентест	«Можем ли мы взломать этот процесс?»
Анализ защищённости	«Какие уязвимости и слабые места у нас есть?»
Red Team	«Смогут ли атакующие пробиться, противодействуя защите?»
Аудит	«Соответствуют ли процессы установленным требованиям?»
SOC	«Что происходит в инфраструктуре прямо сейчас?»
Compromise Assessment	Есть ли признаки того, что инфраструктура уже скомпрометирована или была скомпрометирована?»

Фокус на поиске фактов и артефактов уже состоявшейся или продолжающейся компрометации

Compromise Assessment

Ampire 360°

Выявление следов компрометации



Углубленная проверка ИТ-инфраструктуры Заказчика для выявления признаков скрытого или ранее незамеченного компрометационного воздействия, а также оценки устойчивости организации к киберугрозам

Своевременное
обнаружение киберугроз

Полноценная проактивная
защита инфраструктуры

Снижение рисков
компрометации

Минимизация последствий
возможных инцидентов ИБ

Минимизация проведения
повторной атаки

Как проходит проверка

1 Границы

Определение границ исследования, используемых систем хранения

2 Данные

Сбор и обработка имеющихся данных

3 Поиск

Поиск индикаторов компрометации

4 Проверка

Проверка связей обнаруженного индикатора компрометации

5 Масштаб

Определение масштаба полученного доступа, учётных записей, процессов

6 Результат

Оформление выводов, перечень обнаруженных индикаторов компрометации, рекомендации

От общего к частному – и обратно

1 Вся доступная сеть

Редкие домены и необычные связи

2 Конкретный клиент

IP-адрес + время + история

3 Устройство и процесс

Имя узла, пользователь, цепочка запуска

4 Обнаружение IoC

Происхождение, закрепление, действия

5 Повторный поиск по всей сети

Другие узлы и способы доступа

Сужаем область поиска,
пока не получим
цепочку инцидента

Затем ищем её элементы
во всей доступной
инфраструктуре.

Шаг 1. Необычные запросы DNS

01	Time	ClientIp	QueryName
02	02:20:59	10.24.8.14	intranet.corp.example
03	02:21:03	10.24.8.73	updates-sync.example
04	02:31:08	10.24.8.73	updates-sync.example
05	02:41:11	10.24.8.73	updates-sync.example
06	02:51:14	10.24.8.73	updates-sync.example

08 QueryType: A Rcode: NOERROR

09 Answer: 203.0.113.48

10

11 За 30 дней: 1 клиент для этого домена

12 Первый запрос в доступных данных: 16.09.2026

Один клиент обращается к новому для компании домену примерно раз в 10 минут.

Далее вопрос: кто использовал адрес 10.24.8.73?

Периодические DNS-запросы задают версию для проверки. Соединение проверяем отдельно.

Шаг 2. Установление конкретного сервера

История адресации и контрольное событие / Сопоставление на 16.09.2026, 02:21:03 UTC+3

01 История адресации IPAM

02 Address: 10.24.8.73
03 HostName: APP-SRV-17
04 Assignment: static
05 ValidFrom: 2026-09-01T00:00:00+03:00
06 ValidTo: null (назначение действует)
07 AssetId: VM-00417
08

09 Контроль по Sysmon 3

10 Computer: APP-SRV-17.corp.example
11 UtcTime: 2026-09-15 23:21:04.221
12 SourceIp: 10.24.8.73

История адресации и событие на узле указывают на сервер APP-SRV-17.

Вопрос: какой процесс создал соединение?

IP-адрес связываем с устройством на время события, затем проверяем вторым источником

Шаг 3. Установление взаимосвязей между соединением и процессом

APP-SRV-17 / Microsoft-Windows-Sysmon/Operational / UtcTime в UTC

```
01 EventID: 22      2026-09-15 23:21:03.012
02 QueryName: updates-sync.example
03 ProcessGuid: {8d3b5b0a-2d20-68c8-8f01-000000000a00}
04
05 EventID: 3       2026-09-15 23:21:04.221
06 ProcessGuid: {8d3b5b0a-2d20-68c8-8f01-000000000a00}
07 Image: C:\ProgramData\VendorUpdate\agent.exe
08 User: CORP\vendor.ops
09 Protocol: tcp
10 DestinationIp: 203.0.113.48
11 DestinationPort: 443
12 Initiated: true
```

Один ProcessGuid
связывает
DNS-запрос и соединение
с agent.exe на сервере.

**Далее: кто вошёл
и запустил программу?**

События связывают действие с процессом

Шаг 4. История доступа к серверу

```
01 VPN      2026-09-15T23:14:08Z
02 user: CORP\vendor.ops
03 remote_ip: 198.51.100.27
04 assigned_ip: 10.88.0.26
05 result: success
06 Security 4624      2026-09-15 23:17:42Z
07 Computer: APP-SRV-17.corp.example
08 TargetUserName: vendor.ops
09 TargetDomainName: CORP
10 LogonType: 10
11 IPAddress: 10.88.0.26
12 TargetLogonId: 0x71A09
```

Адрес VPN-сеанса совпал с источником удалённого входа на APP-SRV-17.

Далее: что произошло в сеансе 0x71A09?

Виден доступ через учётную запись

Шаг 5. Задание и запуск файла

APP-SRV-17 / Windows Security и Sysmon / UTC, фрагменты XML

```
01 Security 4698      2026-09-15 23:20:00Z
02 SubjectUserName: vendor.ops
03 SubjectLogonId: 0x71A09
04 TaskName: \VendorUpdate
05 TaskContent / Triggers: <LogonTrigger>
06 TaskContent / Actions / Exec / Command:
07 C:\ProgramData\VendorUpdate\agent.exe
08
09 Sysmon 1          2026-09-15 23:21:00.108Z
10 Image: C:\ProgramData\VendorUpdate\agent.exe
11 ProcessGuid: {8d3b5b0a-2d20-68c8-8f01-000000000a00}
12 User: CORP\vendor.ops
```

В том же сеансе создано задание VendorUpdate. Журнал процессов подтверждает запуск файла.

Далее: какие дочерние процессы он создавал?

4698 подтверждает создание задания

Шаг 6. Действия найденного процесса

APP-SRV-17 / Sysmon 1, создание процессов / UtcTime в UTC

```
01 2026-09-15 23:22:10.006 EventID: 1
02 ParentImage: C:\ProgramData\VendorUpdate\agent.exe
03 ParentProcessGuid: {8d3b5b0a-2d20-68c8-8f01-000000000a00}
04 Image: C:\Windows\System32\cmd.exe
05 ProcessGuid: {8d3b5b0a-2d62-68c8-9001-000000000a00}
06 CommandLine: cmd.exe /c whoami /all
07
08 2026-09-15 23:22:10.020 EventID: 1
09 ParentProcessGuid: {8d3b5b0a-2d62-68c8-9001-000000000a00}
10 Image: C:\Windows\System32\whoami.exe
11 CommandLine: whoami /all
12 User: CORP\vendor.ops
```

Agent.exe создаёт cmd.exe.
Далее выполняется команда проверки пользователя и его привилегий.

Далее: есть ли такая цепочка на других узлах?

Цепочка подтверждает выполнение команд

Шаг 7. Проверка

05	Признак	Узлов	Объекты
06	Домен	1	APP-SRV-17
07	Файл и задание	1	APP-SRV-17
08	Входы vendor.ops	3	APP-SRV-17
09			OPS-SRV-02
10			BKP-SRV-04

Полная цепочка найдена на одном сервере.
Ещё два сервера требуют проверки.

Кейс: выводы и рекомендации

Установлено

- Несогласованный вход, запуск файла.
- Создание задания и дочерних команд.
- Полная цепочка инцидента на сервере APP-SRV-17.
- Два сервера требуют проверки входов.

Рекомендации

- Изолировать APP-SRV-17.
- Сохранить необходимые следы.
- Завершить подозрительные сеансы.
- Проверить ресурсы, куда имеется доступ с сервера.
- Удалить закрепления.
- Проверить результат.

«Вот инфраструктура — разберись сам» — не сработает!

Ampire 

Заказчик помогает:

- Понять инфраструктуру
- Определить критические системы
- Объяснить особенности инфраструктуры
- Предоставить необходимо данные
- Оперативно уточнять обнаруженные события

Исполнитель:

- Формирует гипотезы поиска
- Проводит технический анализ
- Сопоставляет артефакты
- Ищет признаки компрометации
- Формирует выводы и рекомендации

Чем лучше взаимодействие команд, тем полнее итоговая картина!!!

Мифы о Compromise Assessment

Compromise Assessment
сводится к антивирусной
проверке

Достаточно списка адресов
и контрольных сумм

Если ничего не нашло,
то и взлома не было

Compromise Assessment
и пентест дают один результат

Наличие SOC и SIEM делают
Compromise Assessment
ненужной

Удаление файла и смена
пароля закрывают инцидент

Причины сделать СА



После серьёзного инцидента

Даже если инцидент локализован, злоумышленник может находиться в инфраструктуре или иметь доступ к данным



Изменение ИТ-ландшафта

Крупная трансформация инфраструктуры
Объединение доменов
Миграция в облако
Внедрение новых систем



Объединение команд

Соединение организаций
Подключение к общей инфраструктуре региональных подразделений



Регулярная независимая проверка

Даже при наличии SOC и средств защиты полезно периодически проверять инфраструктуру. Мы советуем раз в квартал

Благодарим за внимание!

Софья Карева
менеджер продукта

Никита Гуцуляк
специалист по реагированию
на компьютерные инциденты

Перспективный мониторинг



Ampire 360°