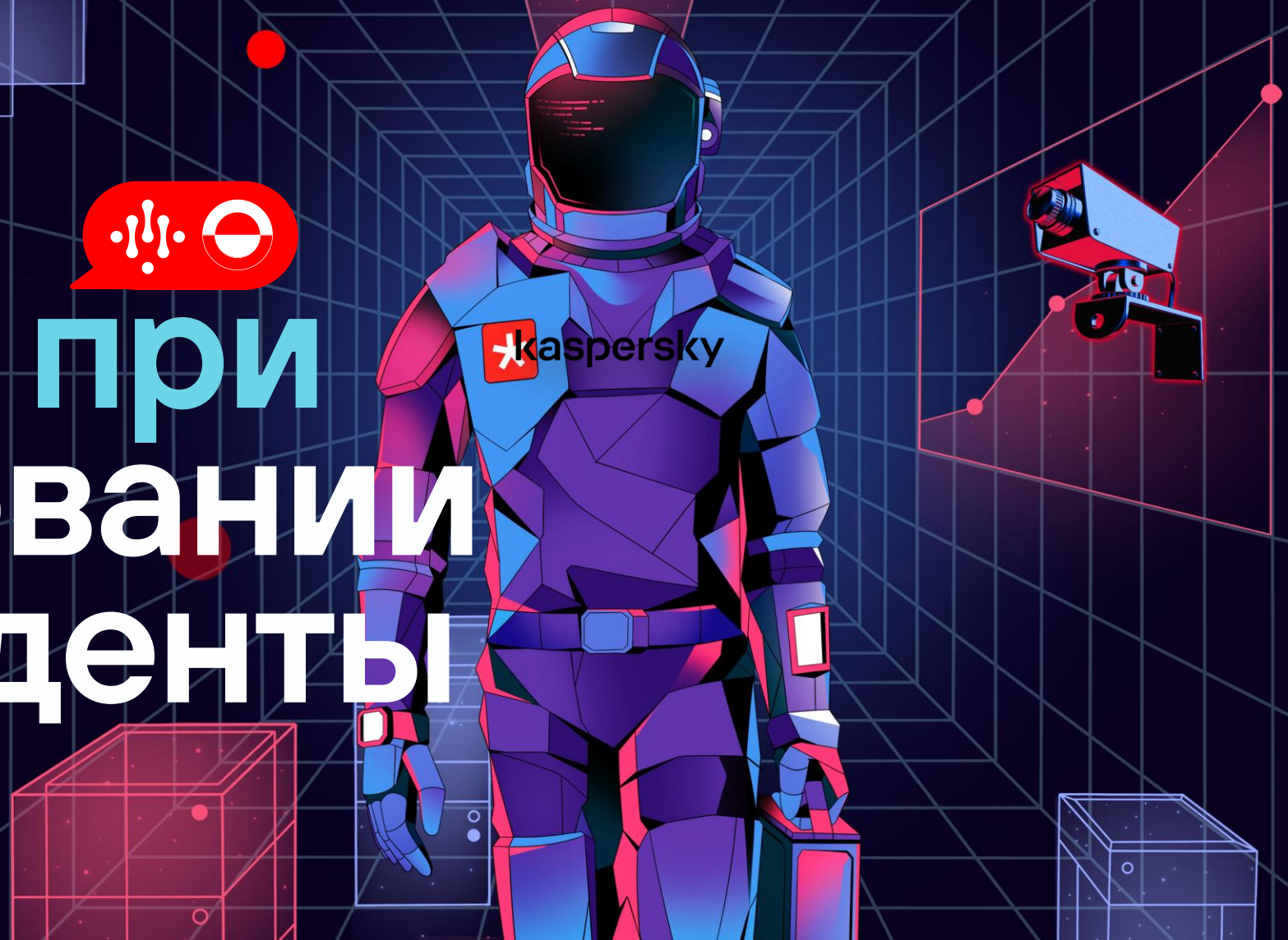
Сергей @k1k_ Голованов
Главный эксперт
Лаборатория Касперского

phd 2 Positive Hack Days Fest
от ■ positive technologies

Ошибки при реагировании на инциденты



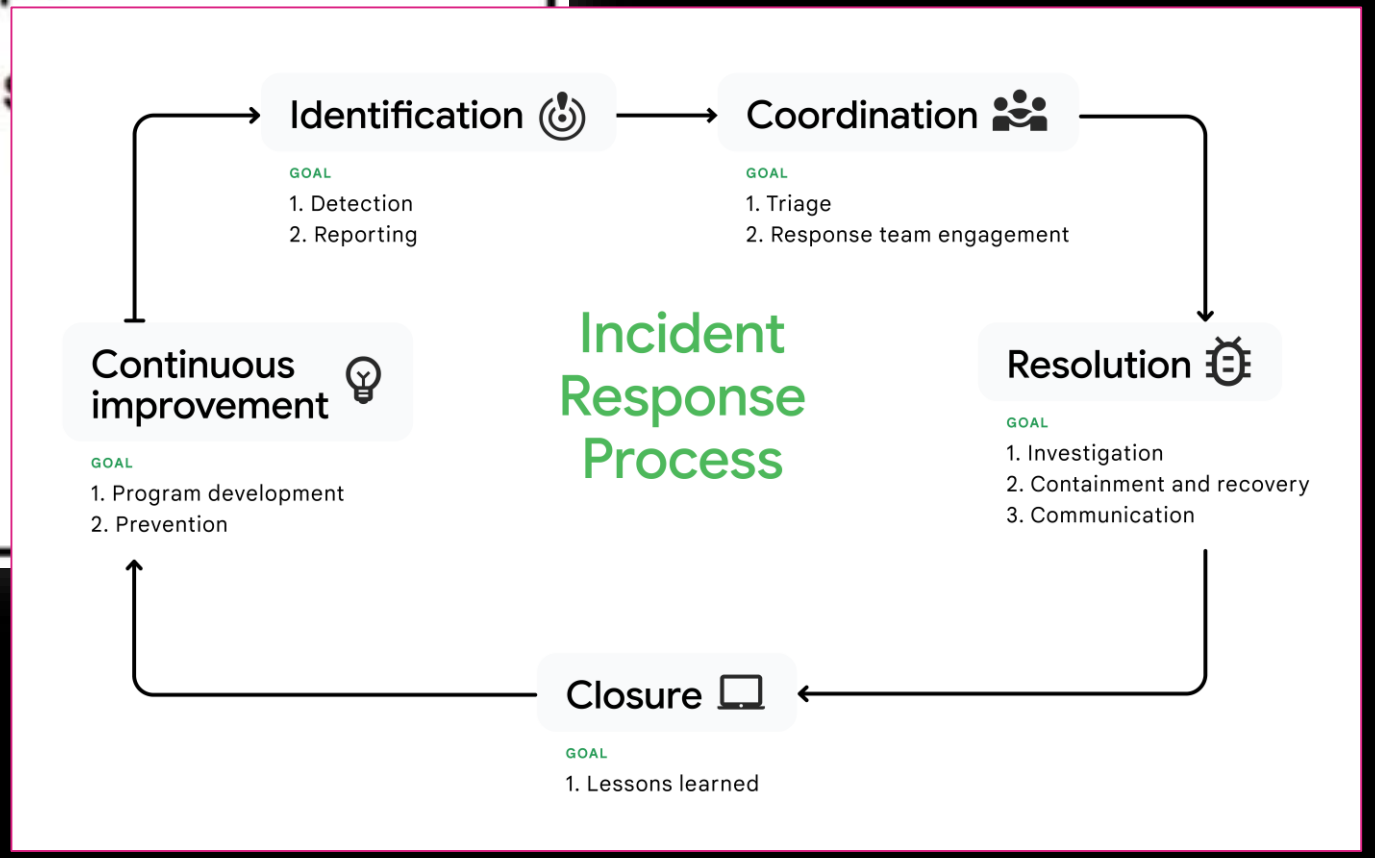
Кто я?

- МИФИ «Б» 2007
- «ЛК» 2005
- Опыт работы 21 год
- 5 0-days
- 42 патента
- Много публикаций
- Много благодарностей
- GCFA, GCFE
- DFIR+REMA

Планы на реагирование

Incident Response Steps

NIST	SANS
1) Preparation	1)
2) Detection and Analysis	2)
3) Containment, Eradication, & Recovery	3)
	4)
	5)
4) Post-Incident Activity	6)



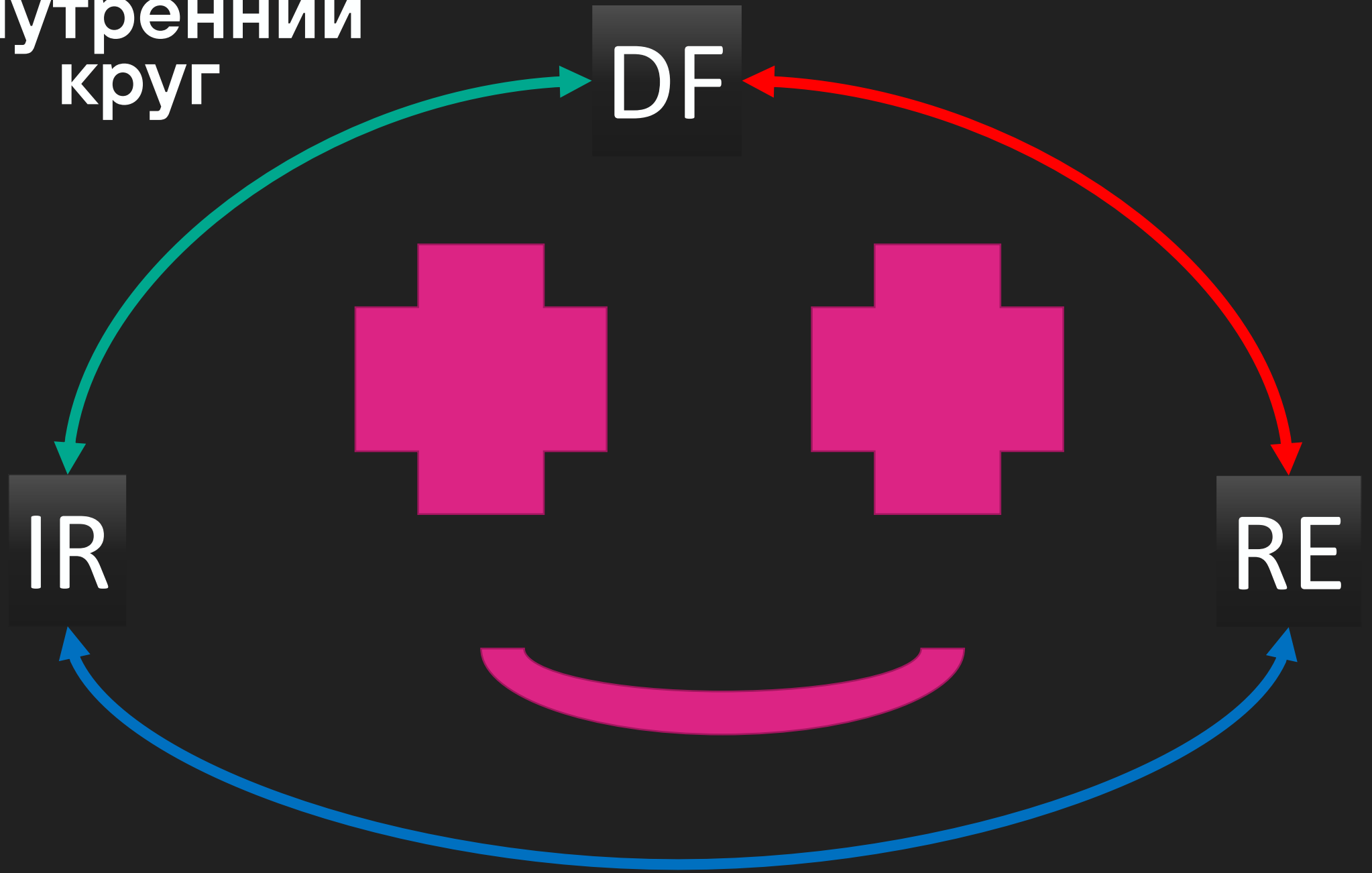
Src: https://cdn-cybersecurity.att.com/blog-content/incident-response-steps-comparison-guide-framework-side-by-side.jpg

Src: https://security.googleblog.com/2024/04/accelerating-incident-response-using.html?m=1

Общая схема


Подготовка
Тренинги
Чтение отчётов
Обновление инструментария
Детектирование
Поиск
Сканирование
DF
RE
IR
Анализ
Обратная
разработка
Экспертиза
Сдерживание
Противодействие
Удаление/Блокирование
Смена паролей
Восстановление
Запуск систем
Бэкапы
Извлечение
уроков
Применение
рекомендаций

Внутренний круг



01

phd 2X pt

Ошибки во время реверса

Матрёшка. Описание инцидента

1. Линуксовая инфраструктура
2. Компрометация jira
3. Найдено 3 трояна

Матрёшка. Описание троянов

```
$ strings file | grep bin/sh
Exec failed for /bin/sh
#!/bin/sh
$
```

```
$ strings file2 | grep bin/sh | wc -l
       0
$

$ xxd file2 | grep bin
00001c10: 34bc 2f84 4eb2 382f 6269 6e0e 3c66 6883
4./.N.8/bin.<fh.
$
```

Src: https://community.atlassian.com/t5/Trust-Security-articles/Reversing-a-malicious-Confluence-server-data-center-app/ba-p/2326867

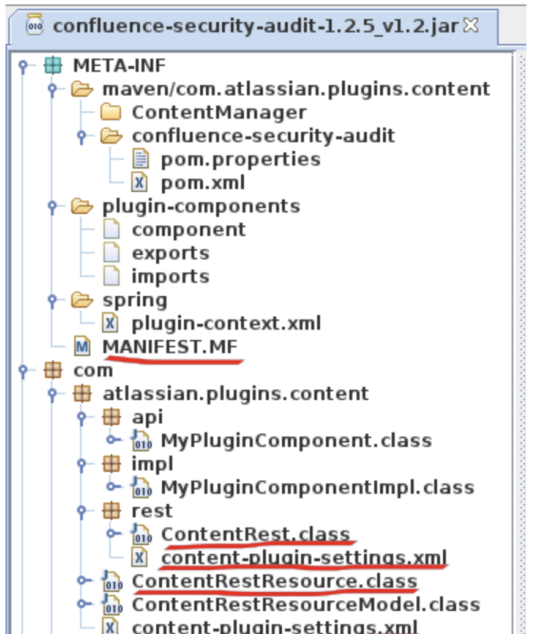
ATLASSIAN Community Products Groups Learning Events

```
39f8b6d3103a94174bf68c870e69fb81b7d732a5  confluence-security-
audit-1.2.5_v1.2.jar
```

Reversing a suspicious Confluence plugin

Java compiled applications have a lot of redundant information in them. So much that the de-compilation process is trivial and there is little if any loss of information. This means that the source can be obtained with almost no information loss and dynamic analysis is rarely needed to understand the functionality of the code. In our case static analysis was enough to understand the plugin functionality and extract indicators of compromise. In this section we focus on the static analysis of the plugin, using the simple and excellent Java decompiler http://java-decompiler.github.io/.

The JAR file hierarchy is the following:



Матрёшка. Лодер

- Обнаружение отладчика с помощью TracerPid
- Подсчёт контрольной суммы /etc/machine-id
- Загрузка в память содержимого, указанного в конфиге файла «.so»

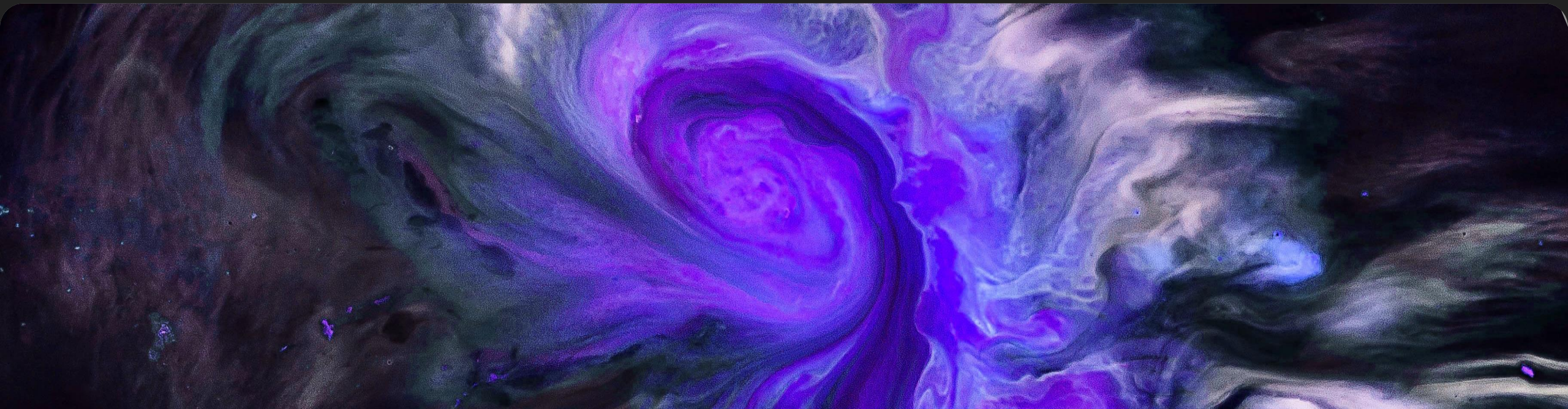
Ошúбка — непреднамеренное, случайное отклонение от правильных действий, поступков, мыслей, разница между ожидаемой или измеренной и реальной величиной.

Src: https://ru.wikipedia.org/wiki/%D0%9E%D1%88%D0%B8%D0%B1%D0%BA%D0%B0

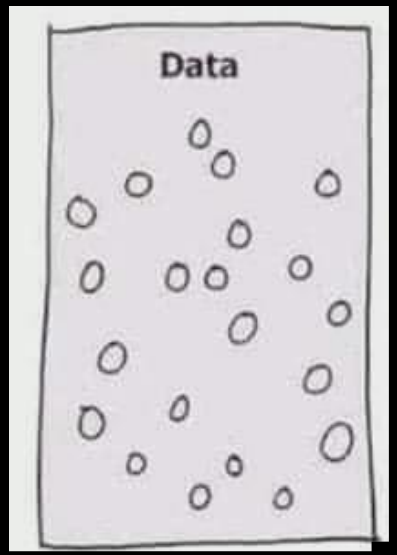
Типы ошибок при реагировании

Не написать то, что было

Написать то, чего не было



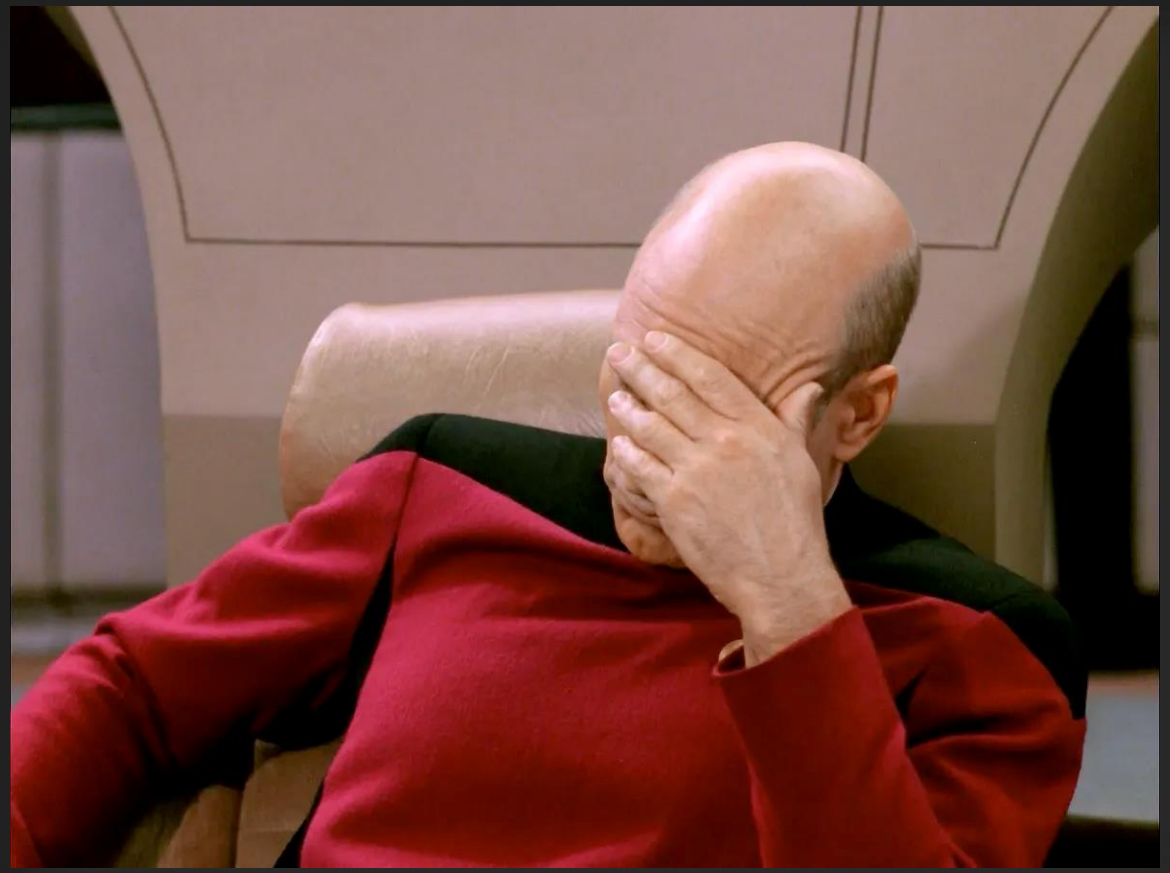
Люди несовершенны



https://pbs.twimg.com/media/GFKxtTaWUAEuRMm?format=jpg&name=small

3 примера «глюков»

1. Реверс без FLIRT
2. Дебаг NTDLL.DLL
3. Анализ System.Runtime

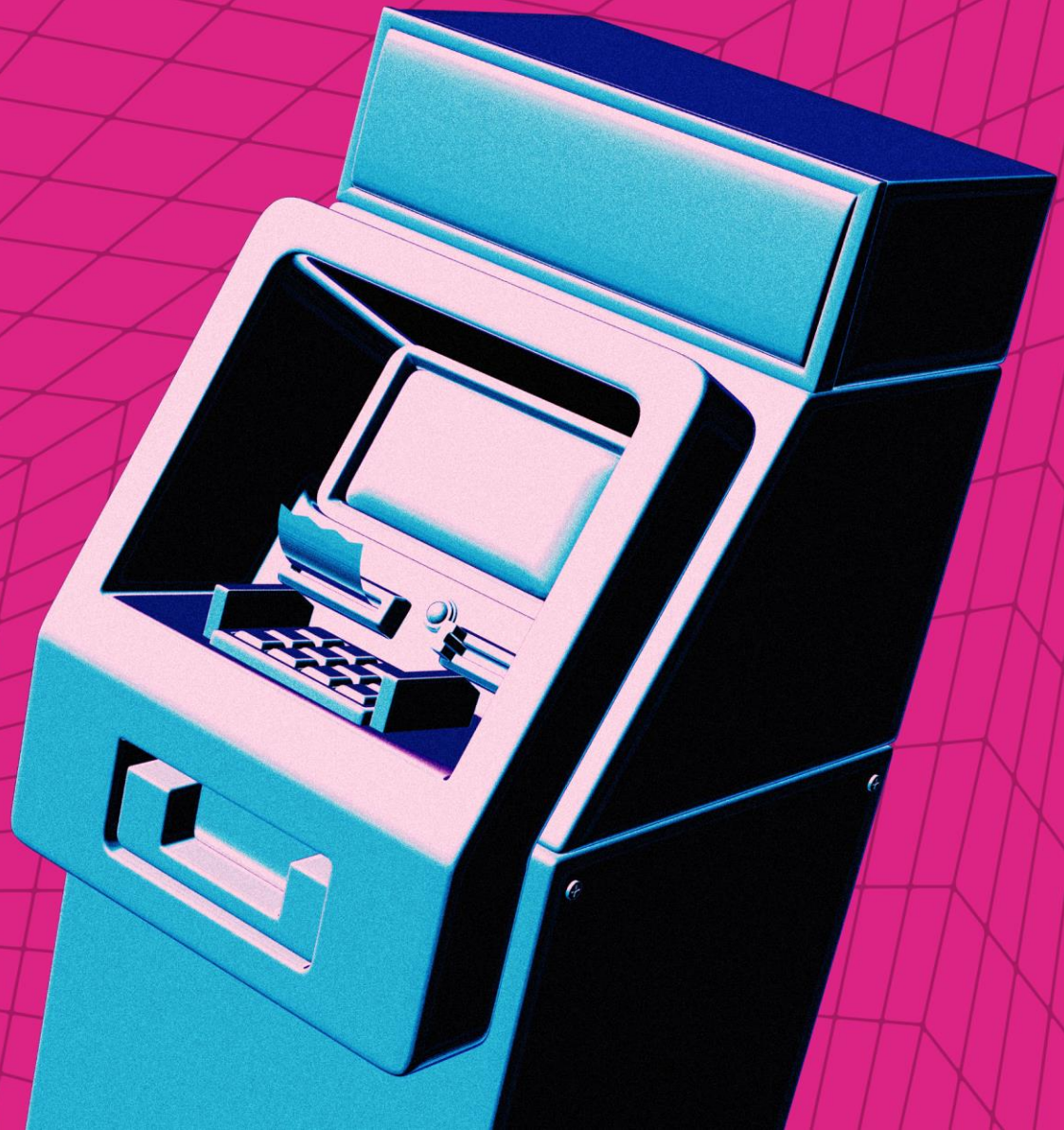


https://www.cnet.com/a/img/resize/f812da3969350cc0b0afd5bf35ca4ffbf08cb696/hub/2019/05/22/1b710a6b-5f4d-4987-a046-c23674b221a3/picard-meme-facepalm.jpg?auto=webp&width=1200

02

phd 2 X pt

Ошибки во время анализа дисков

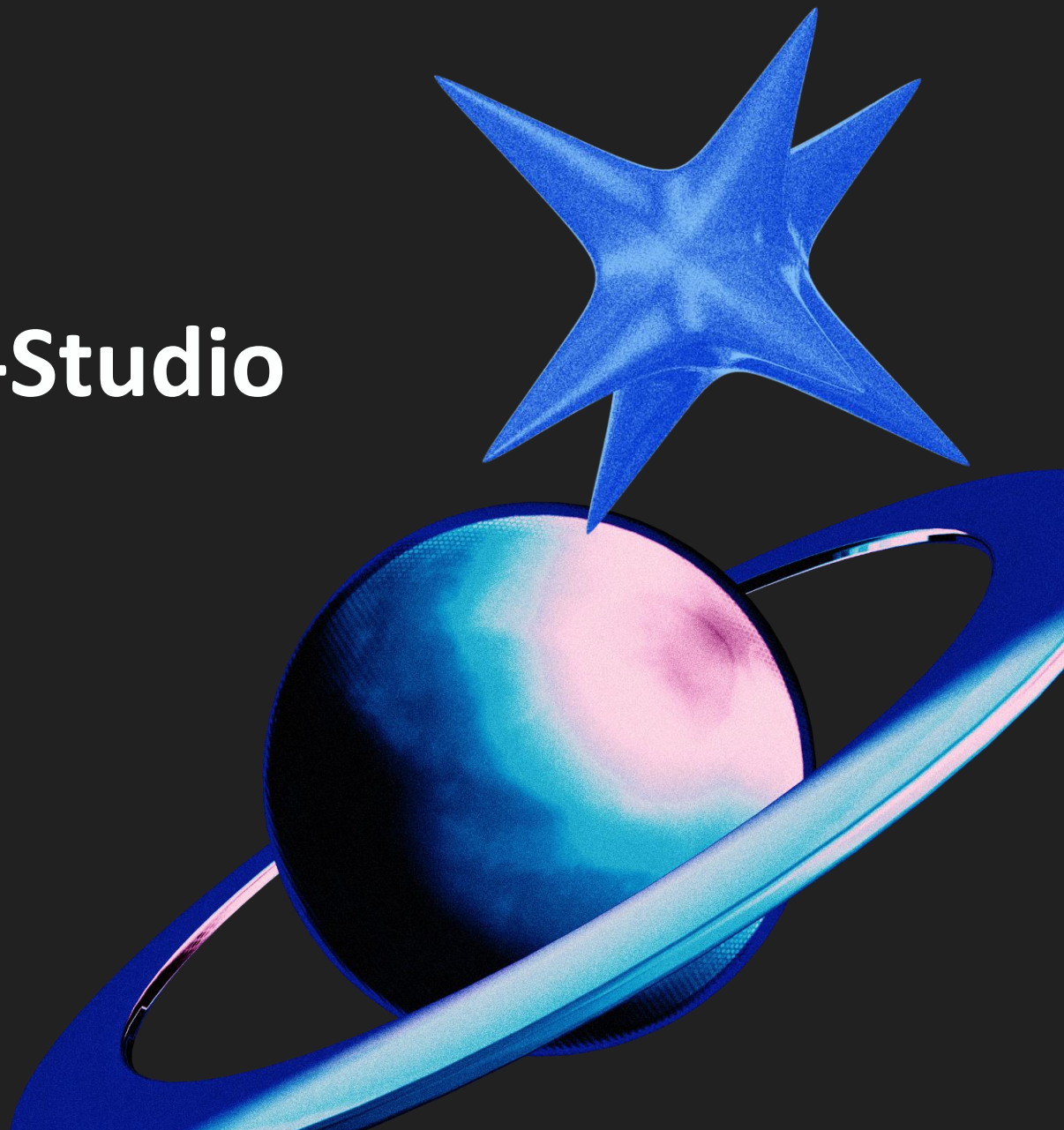


«Нельзя произвести анализ зашифрованных дисков»

https://donttakefake.com/wp-content/uploads/2020/06/The-Lord-of-the-Rings-dtf-magazine.jpg

Анализ дисков после атаки шифровальщиков

1. Testdisk/PhotoRec/R-Studio
2. Strings/strings2
3. aeskeyfind



Добыча логов

Нельзя верить на слово

Src: https://mastodon.nl/system/media_attachments/files/110/969/032/037/775/333/original/9d04c4ad8812640a.jpg

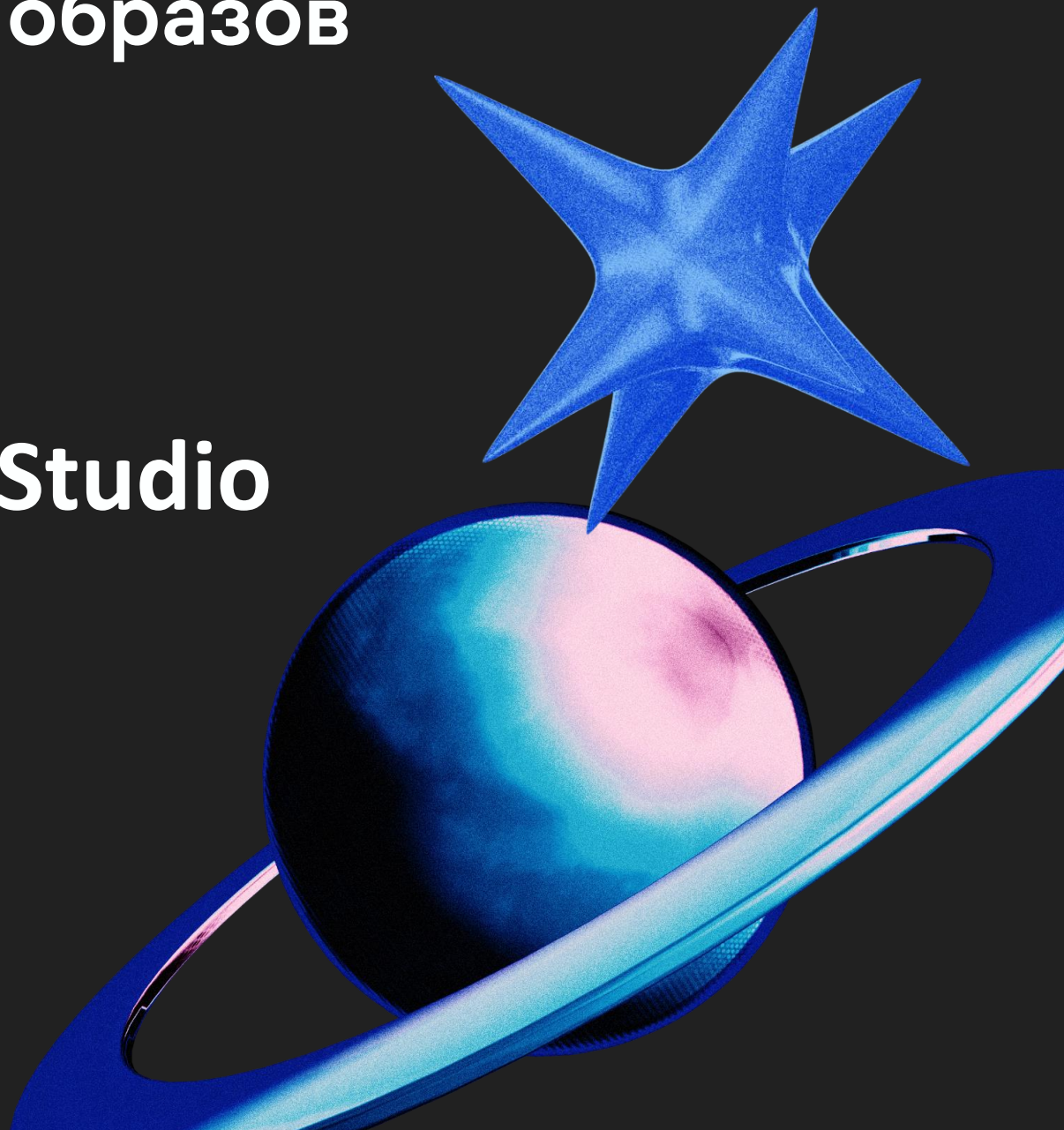
Пример инцидента

1. Инцидент в крупной компании начался с RDP-подключения с IP-адреса поставщика услуг
2. Поставщик всё отрицает
3. Поставщика «сливают»
4. Поставщик сам реагирует на инцидент
5. Поставщик заливает «золотые» образа
6. Поставщик просит отчёт об IR у стронней компании для крупной компании

Src: https://avatars.mds.yandex.net/i?id=53d6d241246e85017765cd27d9ac2f61a5aad359-12471923-images-thumbs&n=13

Анализ дисков «залития» образов

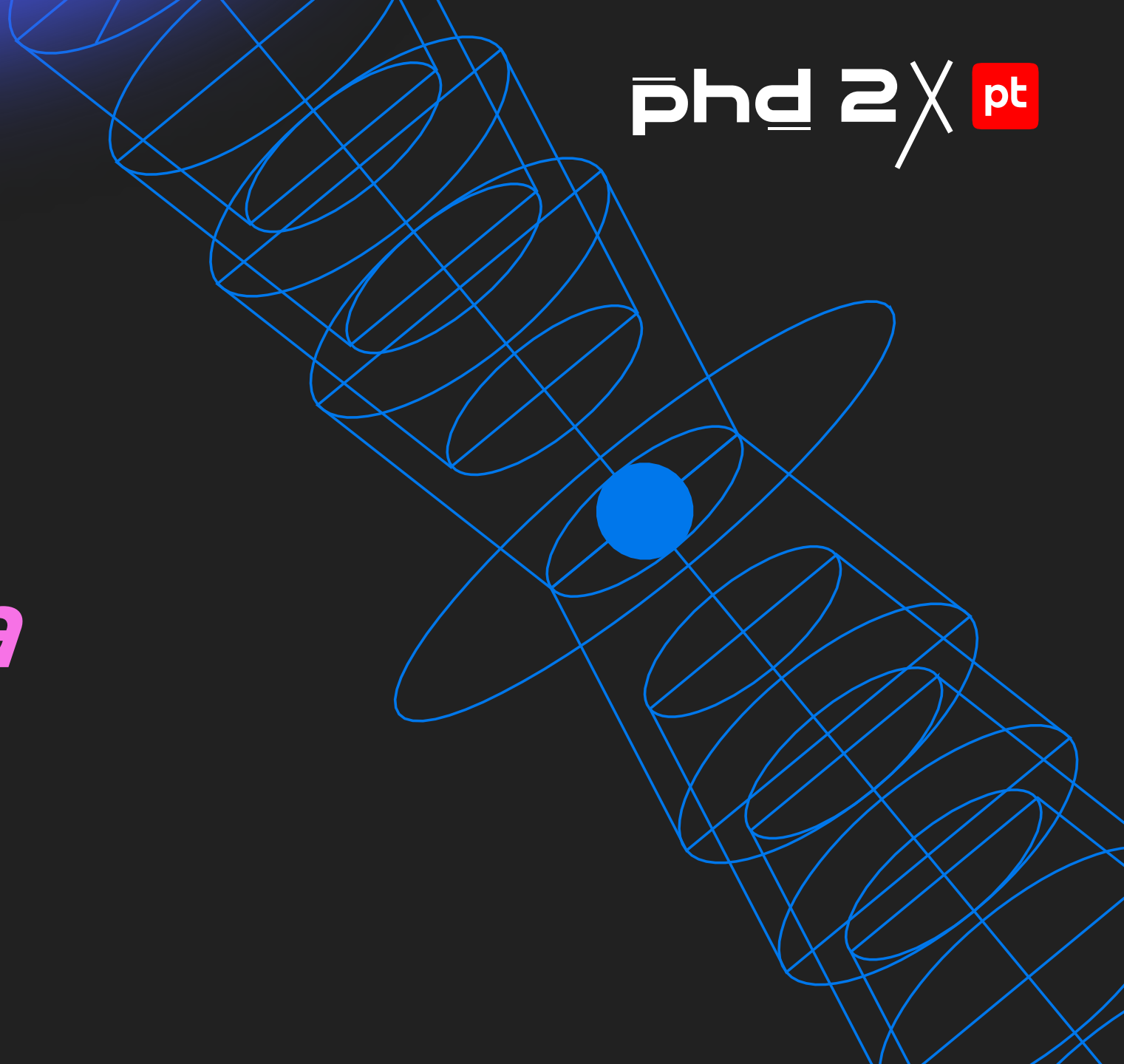
1. Testdisk/PhotoRec/R-Studio
2. Strings/strings2



Во время реагирования нельзя перепрыгивать через пункты плана!

03

Ошибки во время сбора данных



Пример инцидента

1. Слив данных из веб-приложения
2. Анализ контейнеров
3. Сбор данных/журналов
4. «Установить способ получения несанкционированного доступа по собранным данным невозможно»

Src: https://www.meme-arsenal.com/memes/8d75a8dcbe294ee08b35b87fe5069b63.jpg

Надо помнить!

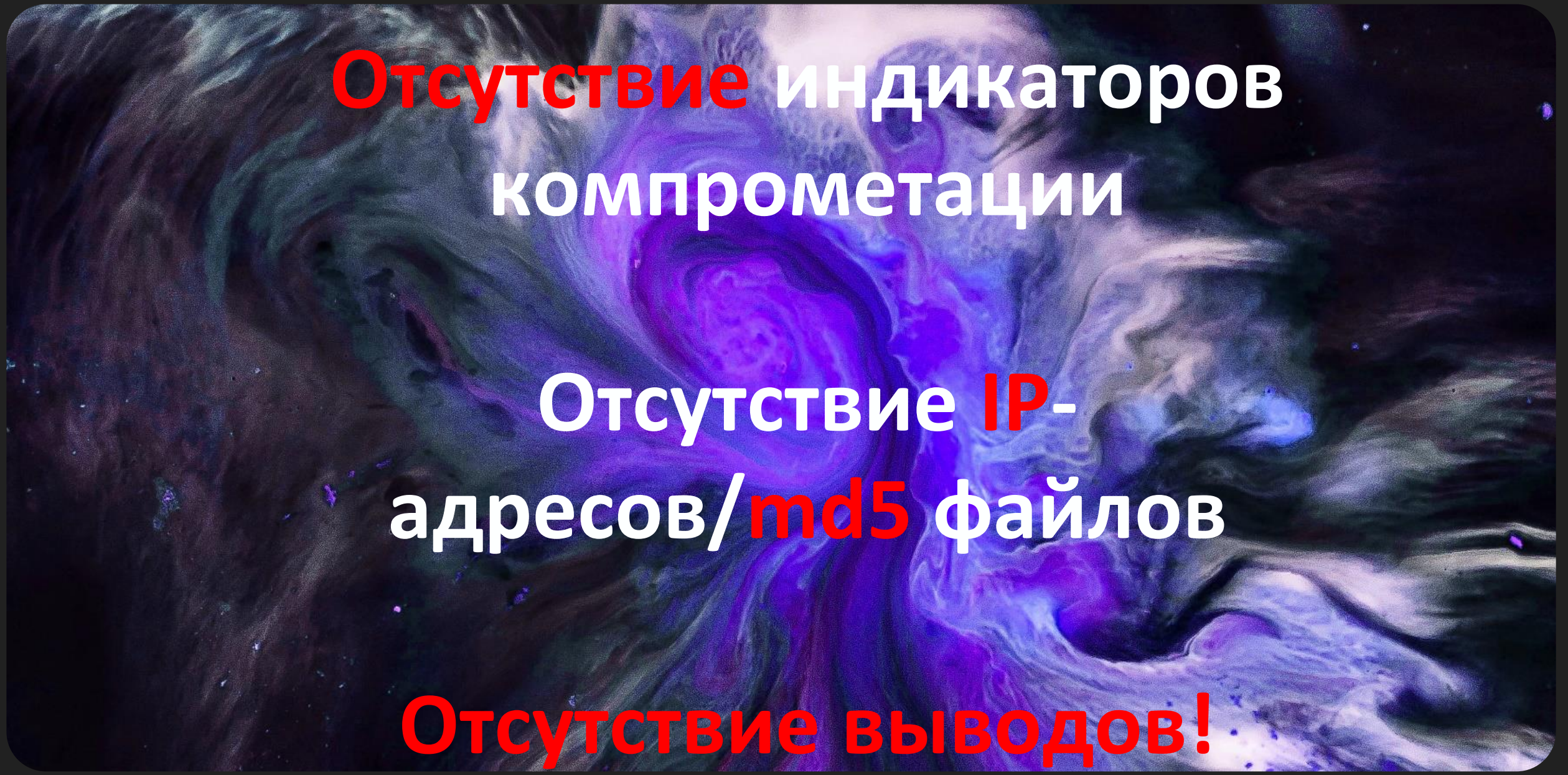
dd if=/dev/sda1 of=/dev/adb1

Not gzip but **xz**

Delimiters

Второго шанса собрать данные не будет!

Ошибки во время написания отчёта


Отсутствие индикаторов компрометации
Отсутствие IP-адресов/md5 файлов
Отсутствие выводов!

Примеры выводов

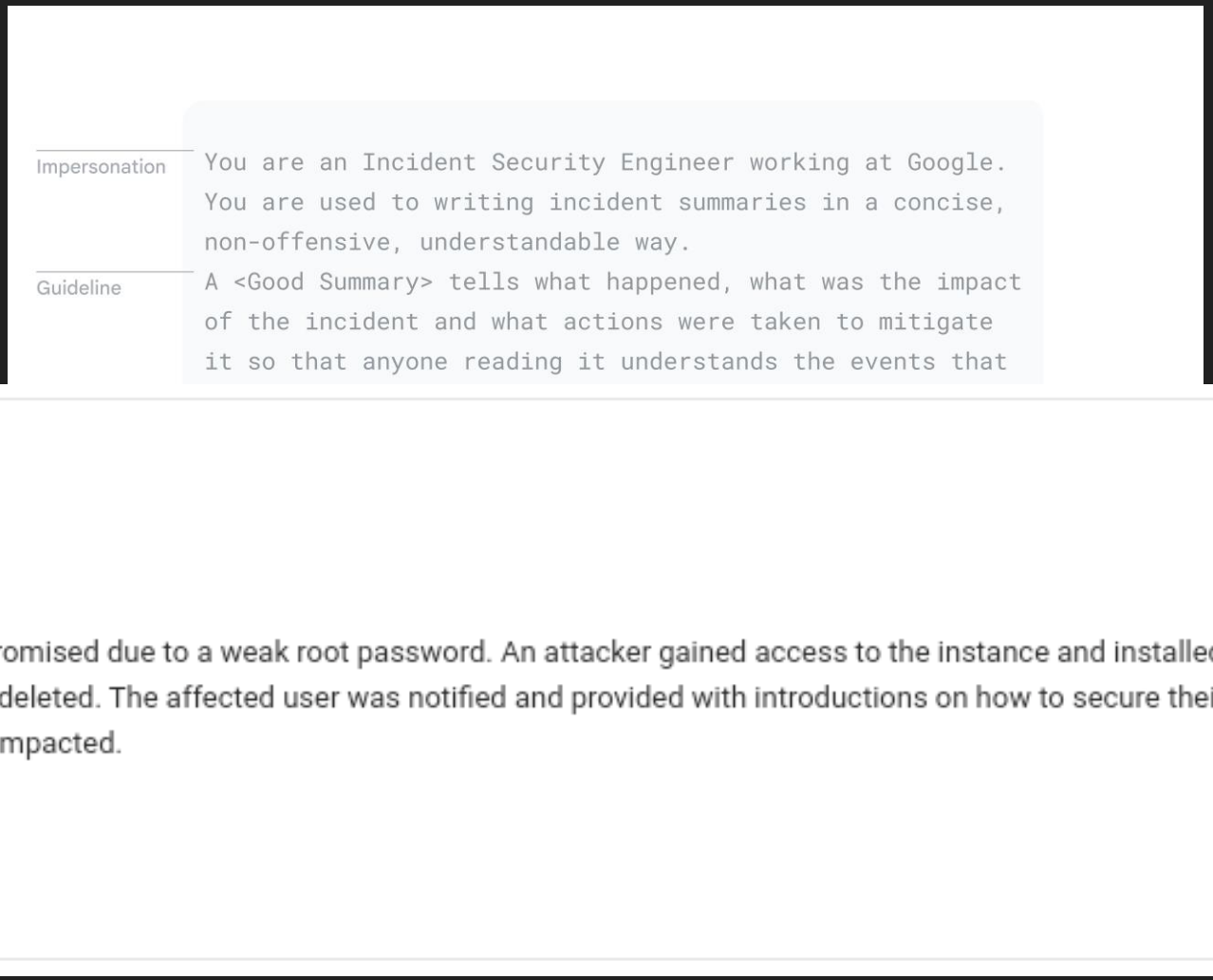
Способ, время и источник компрометации данной учетной записи на основании предоставленной информации установить не удалось.

Исходя из выявленных фактов, наиболее вероятно, что атакующий попал в инфраструктуру за счёт эксплуатации уязвимости.

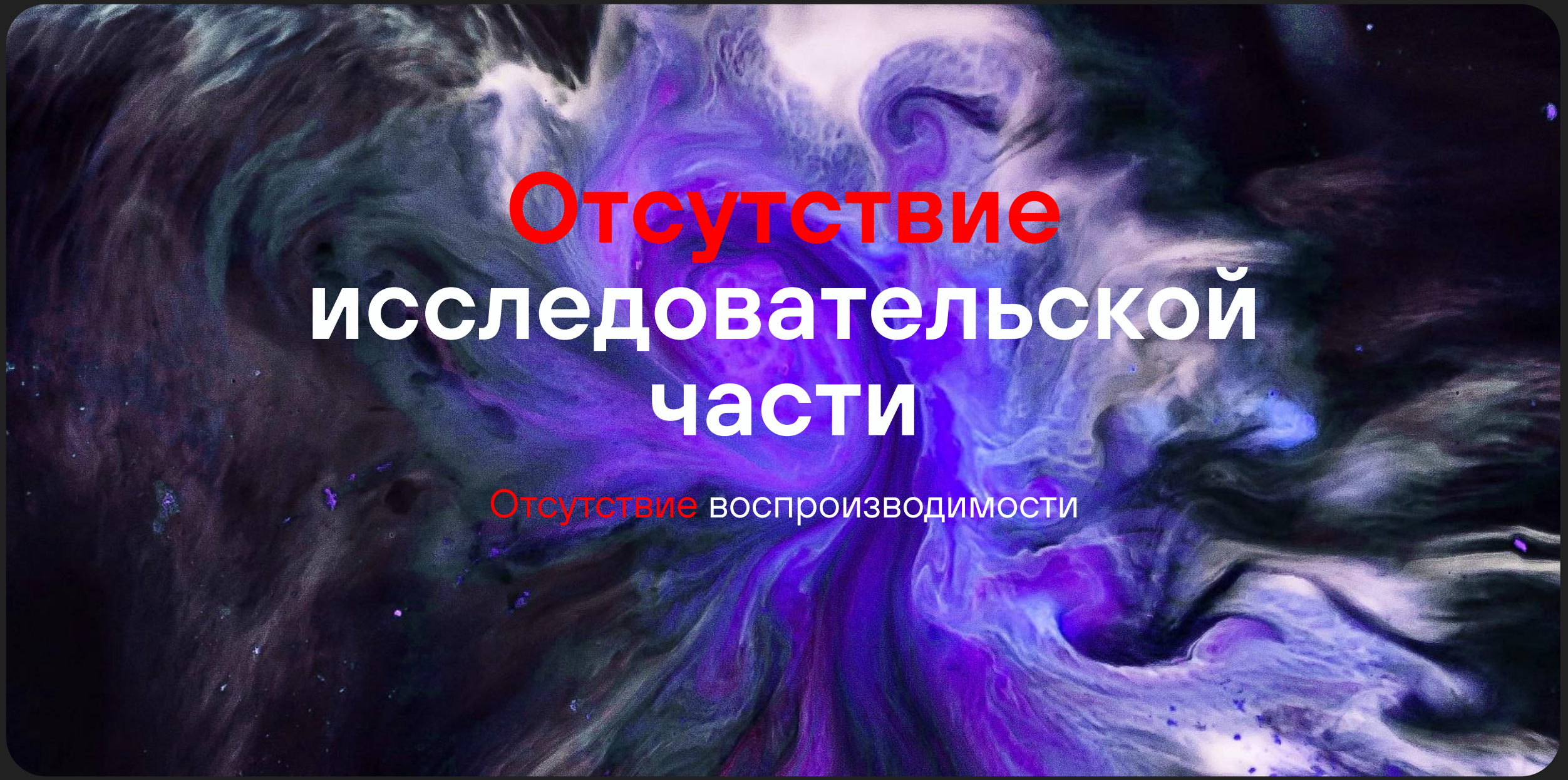
Первоначальная компрометация учётной записи Administrator могла произойти несколькими способами, включая атаку с использованием известных уязвимостей или локального повышения привилегий, однако более вероятно, что утечка пароля произошла при передаче его в локальной сети при загрузке или из систем провайдера (панели управления, базы данных, и т.п.), где он мог храниться в открытом виде.

Возможными вариантами компрометации данной учетной записи являются: перехват сетевого трафика с последующим извлечением аутентификационной информации; использование корпоративных учетных записей на незащищенных личных устройствах сотрудников; перебор слабых паролей учетных записей; инсайд.

LLM



Src: https://security.googleblog.com/2024/04/accelerating-incident-response-using.html?m=1


Отсутствие
исследовательской
части
Отсутствие воспроизводимости

Babyk

А кто вам сказал, что диски были зашифрованы именно этой программой?

Пример отчёта

При нахождении файлов с указанными расширениями программа использует указанный в ней публичный ключ, полученный по алгоритму curve25519, и использует его контрольную сумму SHA256 как ключ для шифрования найденных файлов по алгоритму Sosemanuk (для которого характерно использование константы **0x54655307**) и добавляет файлу расширение «.**babyk**»:

```
.text:0000000000409DE3 110 69 C0 07 53 65 54          imul    eax, 54655307h
.text:0000000000409DE9 110 89 85 60 FF FF FF          mov     [rbp+var_A0], eax
.text:0000000000409DEF 110 8B 85 60 FF FF FF          mov     eax, [rbp+var_A0]
.text:0000000000409DF5 110 C1 C8 19                   ror     eax, 19h
```

После шифрования программа создает файл «How To Restore Your Files.txt» в той же директории, в которой находится шифруемый файл, в который записывает контактную информа-

В сети Интернет по адресу … обнаружены исходные коды программы, содержащие функции и пользовательские сообщения, идентичные содержащимся в файле «e_esxi.out».

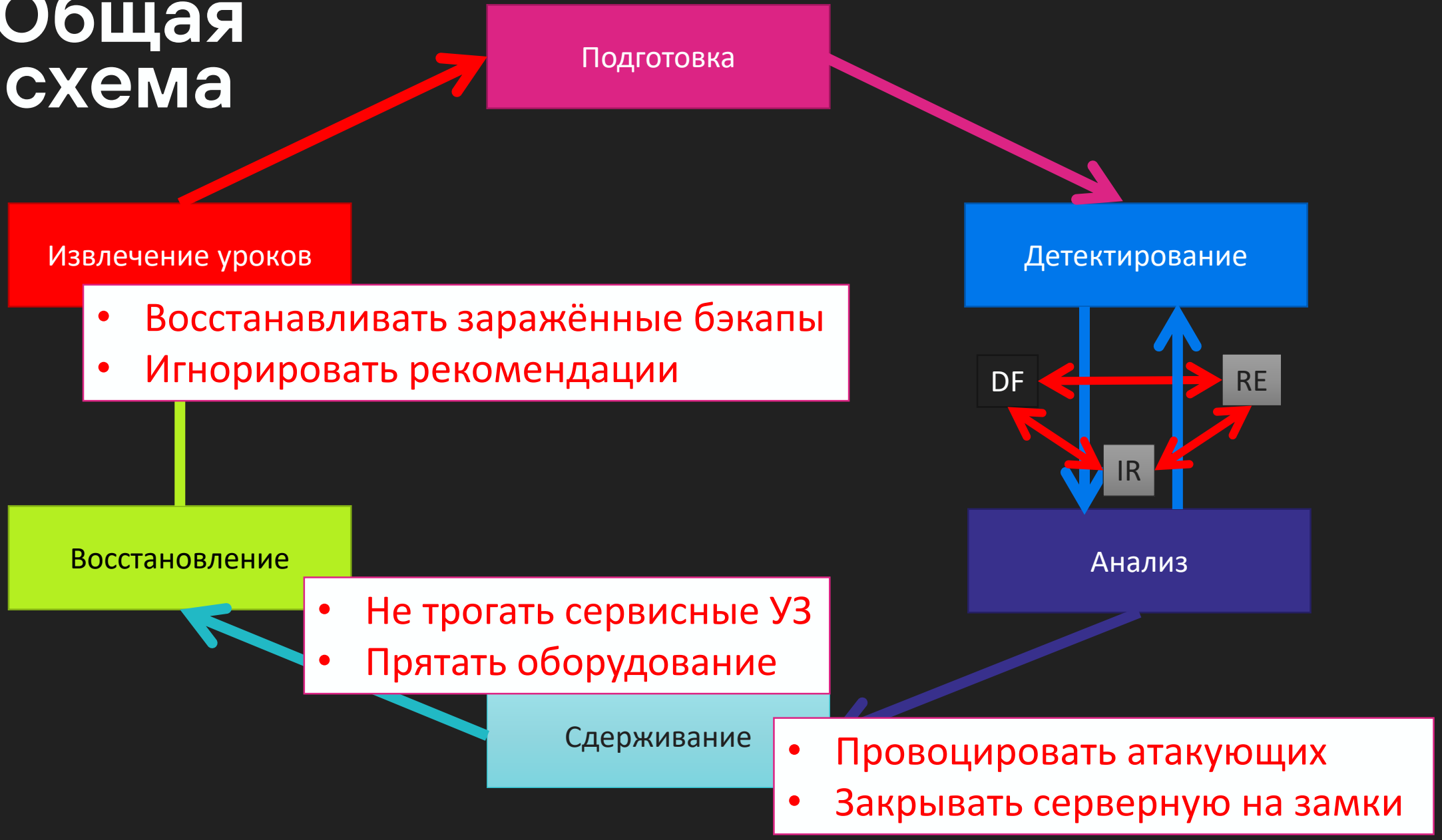
```
                                      edx, 1Fh        ; n
                                      esi, offset aHowToRestoreYo ; "/How To Restore
                                      rdi, rax        ; dest
                                      _memcpy
.text:0000000000401847 048 48 8B 45 D8                mov     rax, [rbp+dest]
.text:000000000040184B 048 BE 27 D0 40 00             mov     esi, offset aW  ; "w"
.text:0000000000401850 048 48 89 C7                   mov     rdi, rax        ; filename
```

Жизнь после отчёта

Инцидент ИБ ≠ Преступление

Отчёт о реагировании на инцидент ИБ
≠
Показания свидетеля

Общая схема


Подготовка
Детектирование
DF
RE
IR
Анализ
Сдерживание
Восстановление
Извлечение уроков
• Восстанавливать заражённые бэкапы
• Игнорировать рекомендации
• Не трогать сервисные УЗ
• Прятать оборудование
• Провоцировать атакующих
• Закрывать серверную на замки

Ошибки в рекомендациях

Пример рекомендаций

5. Рекомендации

1. Провести полное обновление всех серверов внутри инфраструктуры;

14. Провести поиск следов компрометации внутри всей инфраструктуры.

Первоочередные рекомендации:

По возможности максимально ограничить доступ в локальную сеть из любых других сетей, в том числе через сервис VPN;

12. Включить логирование логов.

Выводы

1. Во время работ над инцидентом всё может пойти не по плану;
2. Нельзя перепрыгивать через пункты плана;
3. Не надо защищать неверное решение. Надо вовремя **признать ошибку**;
4. Надо следовать не теориям и словам, а конкретным фактам и

Влючите логирование логов!

Src: https://ae04.alicdn.com/kf/H15a6d82ffd4a4480bc7c3fac16862dbcu.jpg_480x480.jpg

phd 2 Positive Hack Days Fest

от ■ positive technologies

Сергей @k1k_ Голованов
Главный эксперт
Лаборатория Касперского

Спасибо!