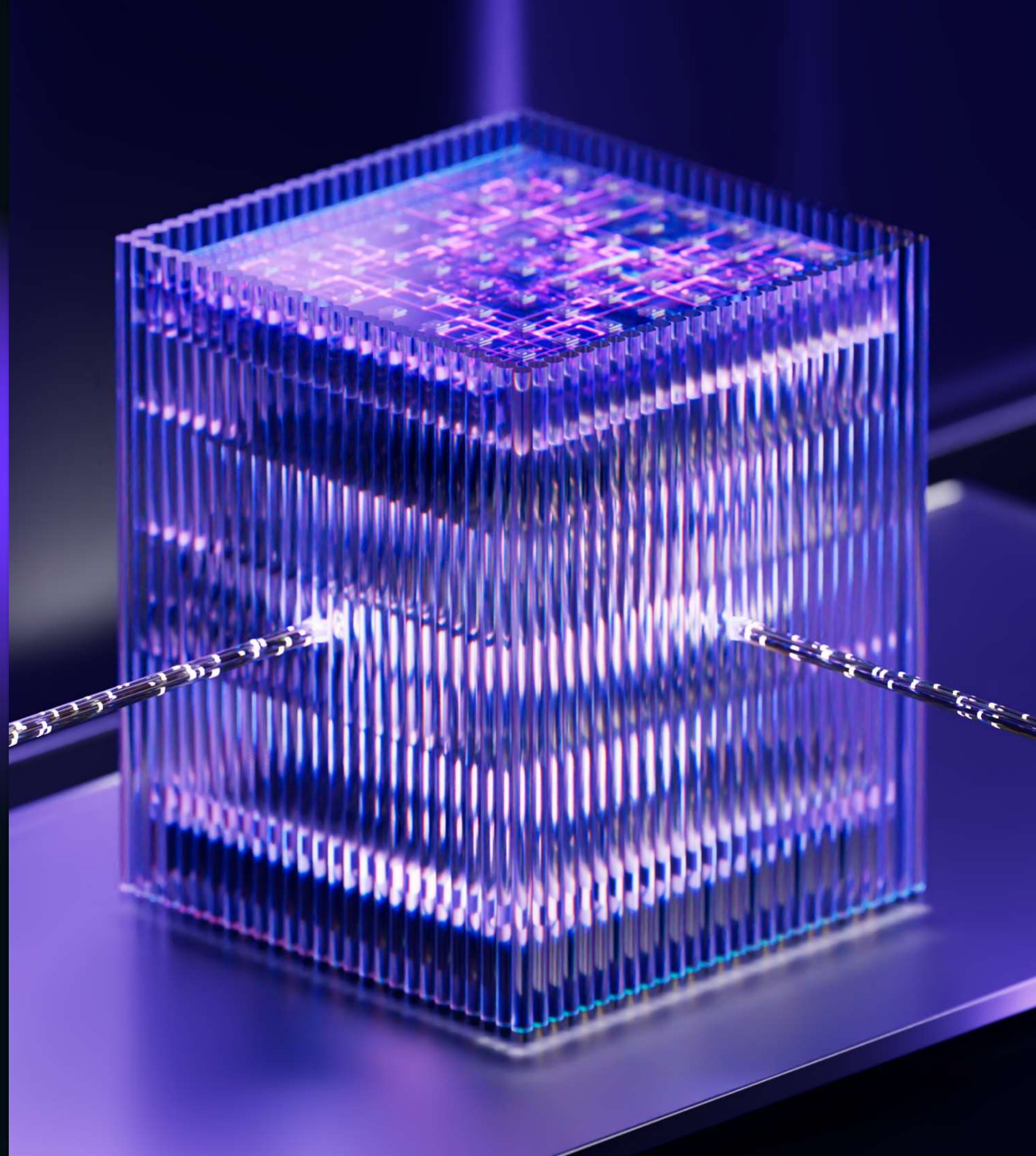
F.A.C.C.T.

F.A.C.C.T.

Российский разработчик технологий для борьбы с киберпреступлениями



F.A.C.C.T.

Судьба – это не дело случая, а вопрос выбора.
Неизвестный автор.

Всё, что случается, имеет причину.
Габриэль Гарсиа Маркес.

О СЕБЕ

F.A.C.C.T.

Каргалёв Ярослав

12 лет

опыт работы в практической кибербезопасности

CERT

возглавлял первый в России частный CERT

DEFENCE CENTER

создал в компании департамент – Центр Кибербезопасности, объединив такие направления как мониторинг, threat hunting и реагирование

Автор

учебных курсов и тренингов на тему работы SOC, мониторинга и реагирования, статей о киберпреступности

Спикер

официальный спикер компании на темы кибератак, фишинга, скама в крипте и фин. мошенничестве

3 СУДЬБЫ - 3 КОМПАНИИ - 3 ИНЦИДЕНТА

F.A.C.C.T.

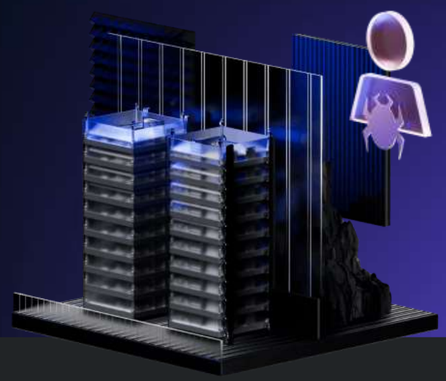
Зашифрована

Цифровая криминалистика

Разработка стратегии восстановления

Мероприятия по восстановлению

Выстраивание новой стратегии ИБ



Атака обнаружена и остановлена

Непрерывный мониторинг инфраструктуры

Удаленное реагирование

Изоляция хостов, блокировка вредоносного процесса

Проблема обнаружена и нейтрализована до ее реализации

Непрерывный анализ периметра

Закрытие потенциальных векторов

Recover & Neutralize | **Detect & Contain** | **Prepare & Prevent**

Панель управления
Угрозы
Утечки
Трояны
Атаки
Опасные IP
Граф
Поддержка
Настройки
Справка

Sticky Werewolf

Опубликовано · En · Rus

MimiStick

Первое появление	19 апр. 2023
Последнее появление	25 сент. 2024
Источник угрозы	Ukraine
Отрасль	Manufacturing · Government and military->Military · Hardware->Satellite communication +27
География	
Теги экспертизы	Unique_data · Windows · RAT +3

Последние угрозы 58

- MimiStick - Найдены новые индикаторы — 26 сент. 2024
- Sticky Werewolf использует обновленные TTPs для установки Quasar RAT в атаках на ОПК России, что подтверждает атрибуцию кампании MimiStick к группе Sticky Werewolf — 26 сент. 2024
- MimiStick - подражатели или очередная эволюция Sticky Werewolf? — 24 сент. 2024

+ Добавить в Ландшафт угроз · 1 · 213

Blackjack

Опубликовано · En · Rus

Gambling Hyena, Lifting Zmiy, Gambling Zealot

Первое появление	22 янв. 2023
Последнее появление	29 авг. 2024
Источник угрозы	Ukraine
Отрасль	Government and military · Messaging and telecommunications · Financial services · Hardware +7
География	
Теги экспертизы	Hacktivism · Leak · Current crisis +9

Последние угрозы 19

- Анализ атакующего BlackJack по данным Kaspersky — 29 авг. 2024
- Анализ атакующего BlackJack (Gambling Zealot) по данным RT-Solar — 06 авг. 2024
- Анализ атакующего BlackJack по данным RT-Solar и новые атаки — 15 июля 2024

+ Добавить в Ландшафт угроз · 76

HsHarada

Опубликовано · En · Rus

Rapture

Первое появление	31 дек. 2022
Последнее появление	13 сент. 2024
Источник угрозы	—
Отрасль	Education · Health care
География	
Теги экспертизы	Ransomware · Cobalt Strike +4

Последние угрозы 7

- HsHarada - Найдены новые индикаторы — 14 сент. 2024
- Активность группировки в августе 2024 — 05 авг. 2024
- Атака HsHarada на компанию из России - февраль 2024 — 14 февр. 2024

-=TWELVE=-

Опубликовано · En · Rus

xtwelvex, twelve_squad, Twelve, Twelfth Wolf, Twelfth Hyena

Первое появление	30 дек. 2022
Последнее появление	15 авг. 2024
Источник угрозы	—
Отрасль	Manufacturing · Energy->Oil and gas · Government and military · Government and military->Government +5
География	
Теги экспертизы	Leak · Hacktivism · Deface +7

Последние угрозы 15

- Unified Kill Chain группировки Twelve — 15 авг. 2024
- Анализ атакующего Twelve по данным RT-Solar — 28 мая 2024
- Удаление канала Twelve в Телеграм — 17 апр. 2024

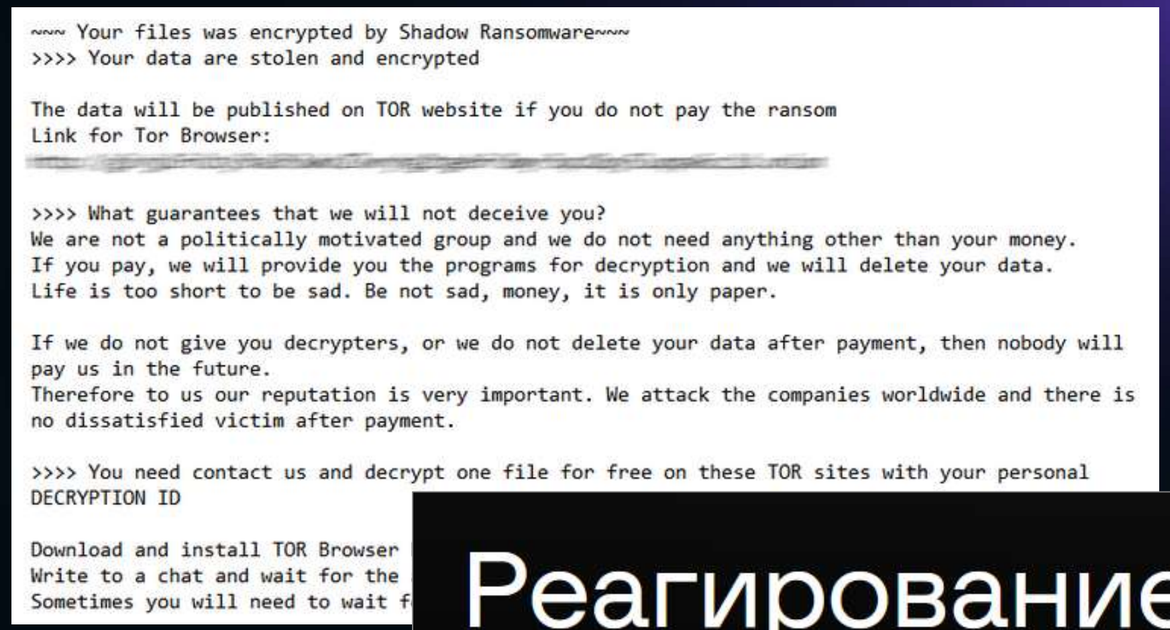
F.A.C.C.T.

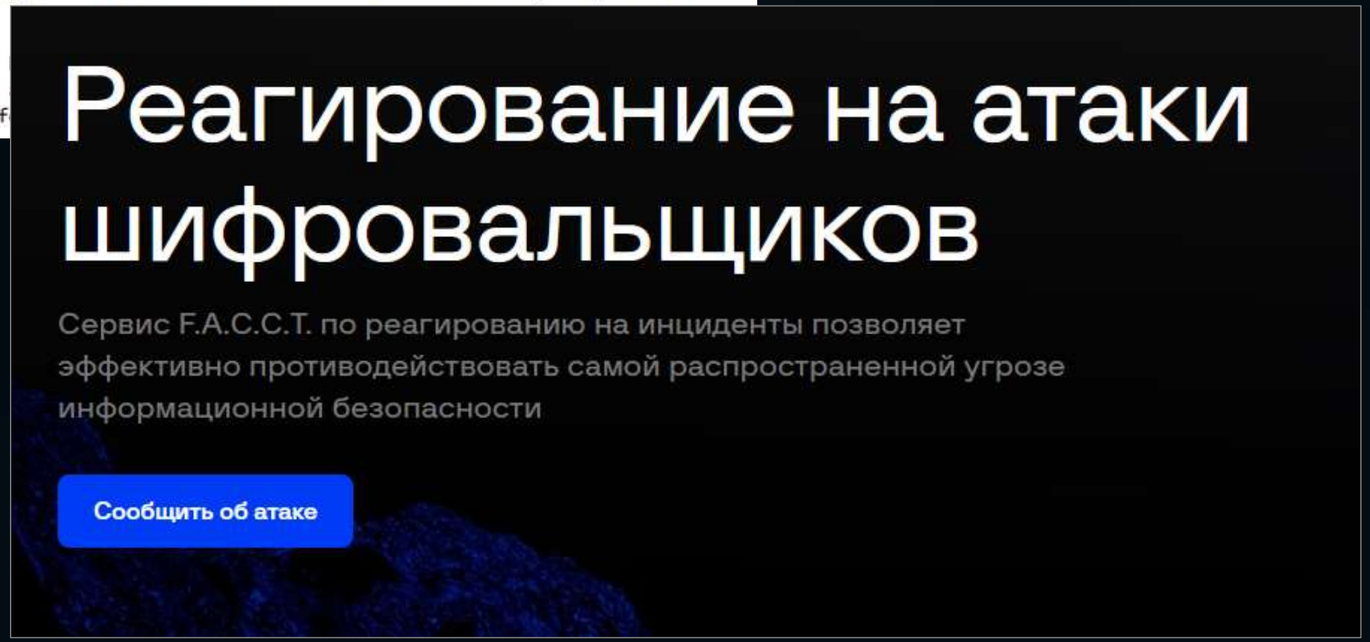
Клиент Первый

Жертва шифровальщиков

ЖЕРТВА ШИФРОВАЛЬЩИКОВ

F.A.C.C.T.





Профайл

Тип инцидента:

Успешная атака шифровальщиком

Воздействие:

Большой объем данных выгружен злоумышленниками

Инфраструктура выведена из строя

Остановка бизнеса, финансовые и репутационный потери.

ЭТАП РЕАГИРОВАНИЯ И ВОССТАНОВЛЕНИЯ

F.A.C.C.T.

Оперативный анализ и локализация инцидента

Сбор и исследование данных с рабочих станций и серверов, задействованных в инциденте

Обнаружение каналов управления злоумышленников и их блокирование

Выявление скомпрометированных устройств

Выявление вектора первоначальной компрометации

Атрибуция злоумышленников

Углубленный криминалистический анализ данных и вредоносного программного обеспечения

Детальный анализ действий атакующих на различных этапах атаки

Исследование обнаруженных образцов вредоносных программ

Выявление скомпрометированной информации

Реконструкция событий инцидента и подготовка отчета

Разработка стратегии восстановления и рекомендаций

Устранение последствий инцидента и эффективное восстановление работоспособности инфраструктуры

Повышение общего уровня защищенности ИТ-инфраструктуры компании

Конфигурирование имеющихся средств безопасности в соответствии с лучшими Практиками

Мониторинг в режиме 24/7

Внедрение F.A.C.C.T. Managed XDR:
Обнаружение нелегитимной активности на конечных точках и вредоносного трафика
Круглосуточное реагирование и локализация возникающих угроз специалистами ЦК F.A.C.C.T.

F.A.C.C.T.

Клиент Второй

Отражение атаки

MANAGED XDR

F.A.C.C.T.

Мониторинг 24/7, проактивный поиск недектируемых угроз и активное реагирование

База данных XDR

F.A.C.C.T. XDR

Защита конечных станций и реагирование

Персональные компьютеры и серверы

Защита корпоративной почты

Вложения, ссылки, фишинг и спам

Анализ сетевого трафика

Мониторинг сети, обнаружение аномалий

Детонация вредоносного ПО

Изолированная среда, анализ файлов и ссылок

MANAGED DETECTION

Сервис круглосуточного мониторинга и анализа подозрительных событий, выявленных решениями F.A.C.C.T.

ЦИКЛ МОНИТОРИНГА ИНФРАСТРУКТУРЫ КОМАНДОЙ ЦЕНТРА КИБЕРБЕЗОПАСНОСТИ F.A.C.C.T:

Благодаря работе с передовыми данным кибербразведки, F.A.C.C.T. вовремя обнаружит и оповестит вашу команду о потенциальной угрозе.

Сосредоточьтесь на важных событиях и реагируйте на них по готовым рекомендациям от команды F.A.C.C.T.

1 Мониторинг событий, на круглосуточной основе командой ЦК F.A.C.C.T.

2 Классификация и анализ для фильтрации ложноположительных срабатываний — менее 30 минут

3 Корреляция связанных оповещений для представления полной картины инцидента

4 Оформление инцидентов и уведомление об опасных событиях с рекомендациями — менее 1 часа

5 Атрибуция выявленной угрозы до известных злоумышленников

← Повторный мониторинг

→ Managed Response

24/7

мониторинг опытной командой Центра кибербезопасности F.A.C.C.T.

менее **30 минут**

триаж каждого алерта и его верификация

менее **1 часа**

предоставление рекомендаций по локализации и устранению угрозы

MANAGED RESPONSE

Сервис оперативного реагирования EDR-решением на выявленные инциденты

ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КОМАНДОЙ ЦЕНТРА КИБЕРБЕЗОПАСНОСТИ F.A.C.C.T:

Обнаруженные на этапах Managed Detection и Managed Threat Hunting инциденты будут остановлены

Специалисты реконструируют жизненный цикл атаки и предоставят рекомендации для предотвращения аналогичных инцидентов.

1. Обнаружение вредоносных событий на этапах Managed Detection & Managed Threat Hunting
2. Оперативное реагирование и локализация инцидента — менее 30 минут
3. Сбор информации с хостов с помощью EDR агентов XDR решения и других инструментов
4. Криминалистический анализ собранных данных экспертами DFIR лаборатории
5. Анализ вредоносного ПО как с помощью функций XDR решения, так и вручную силами специалистов по реагированию
6. Ликвидация последствий и рекомендации по предотвращению использования скомпрометированных хостов потенциальными атакующими

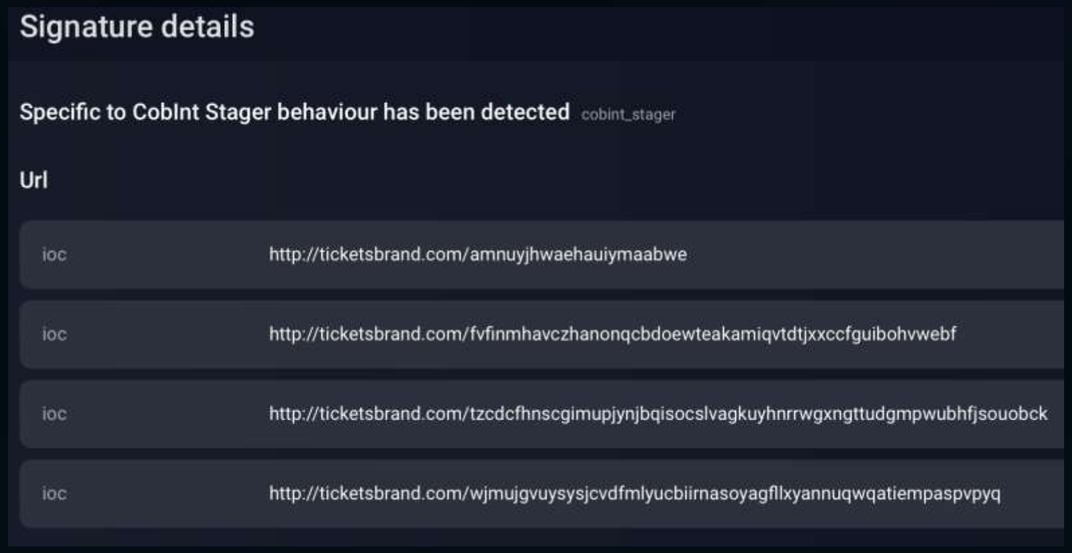
ИДЕНТИФИКАЦИЯ, ЛОКАЛИЗАЦИЯ И ЛИКВИДАЦИЯ ИНЦИДЕНТА

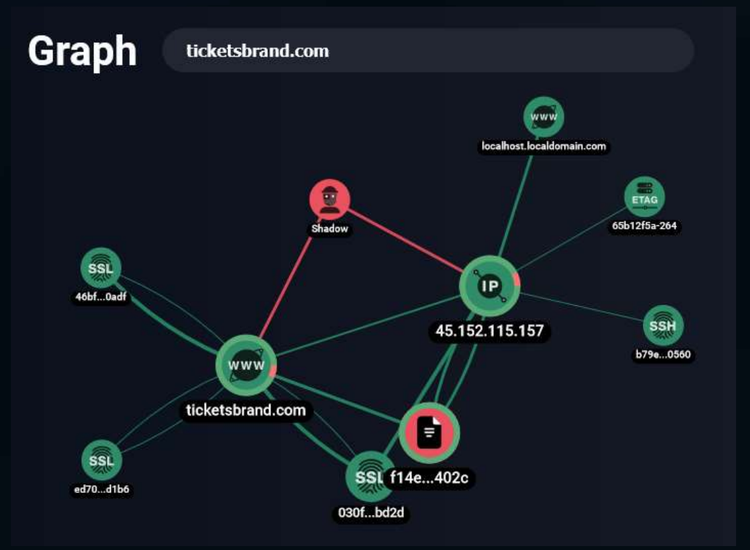
- Установленные причины возникновения инцидента
- Реконструированный жизненный цикл атаки и ход событий на устройствах
- Рекомендации по предотвращению аналогичных атак в будущем

менее **30 минут**
на локализацию инцидента

24 часа
на отчет по инциденту

ОБНАРУЖЕНИЕ И РЕАКЦИЯ





F.A.C.C.T.

Профайл

Тип инцидента:

Обнаружена вредоносная активность

Атрибуция:

Политически и финансово-мотивированная группировка Shadow (Comet, DarkStar) / Twelve

Воздействие:

Скомпрометированные привилегированные УЗ

Закрепление атакующих в инфраструктуре

Разведка и сбор информации

ЭТАП РЕАГИРОВАНИЯ И ЛОКАЛИЗАЦИИ

F.A.C.C.T.

Оперативный анализ и локализация инцидента

Изоляция задействованных в инциденте устройств

Сбор и исследование данных

Выявление скомпрометированных устройств

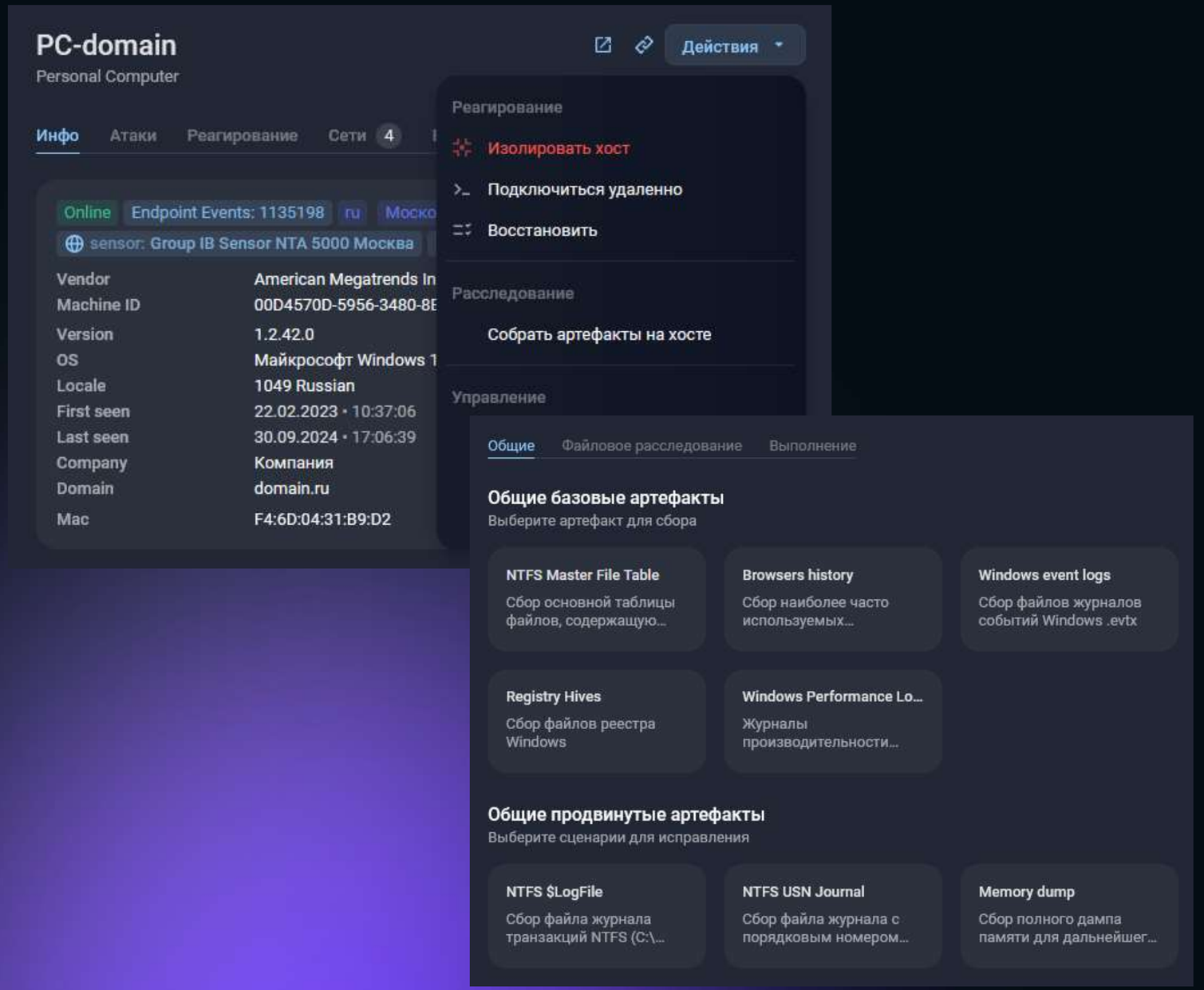
Выявление вектора первоначальной компрометации

Атрибуция злоумышленников

Анализ действий атакующих на различных этапах атаки

Устранения обнаруженных угроз и восстановление

Реконструкция событий инцидента и подготовка отчета



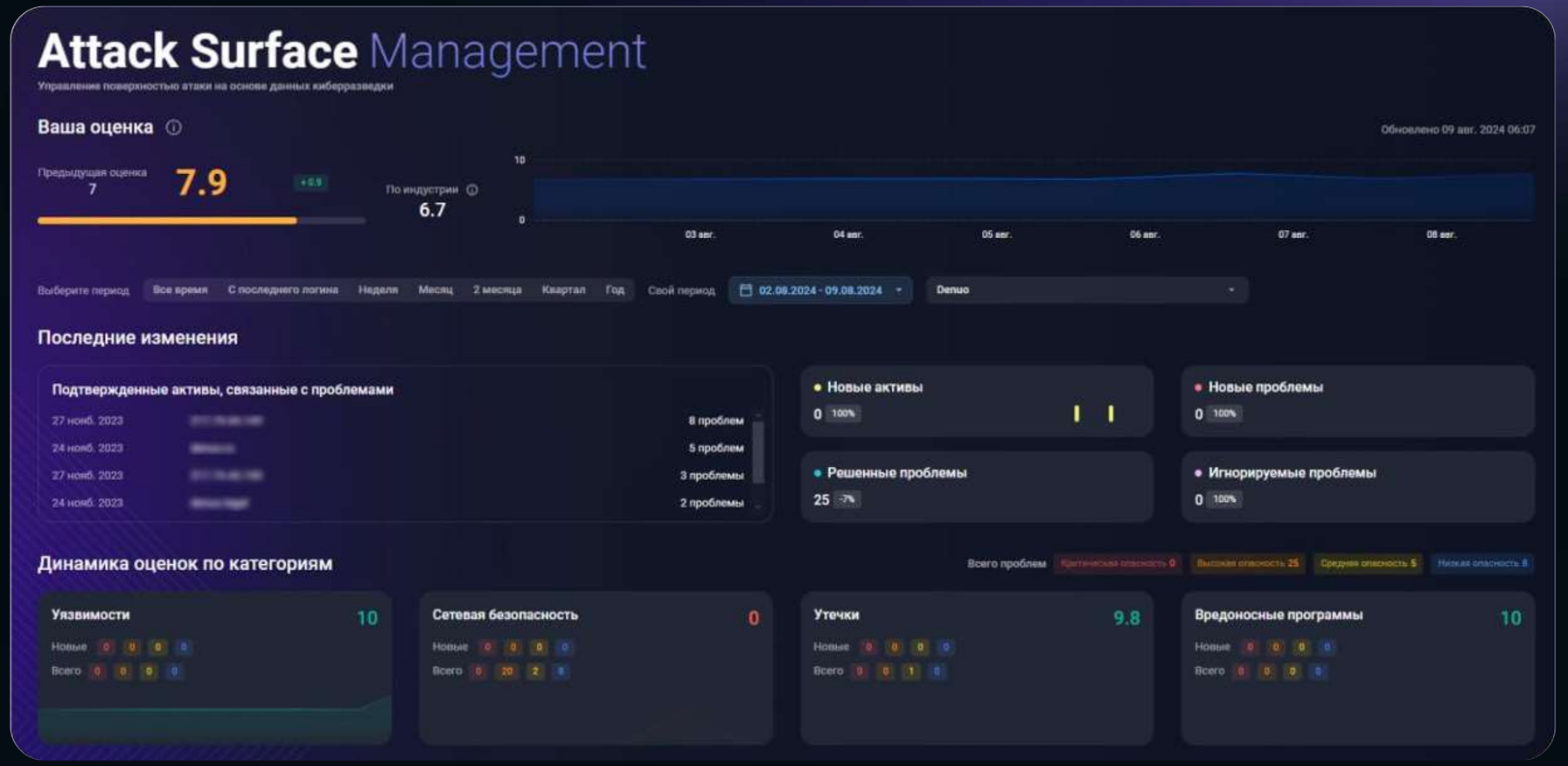
F.A.C.C.T.

Клиент Третий

Предотвращение

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРОБЕЛОВ В ИНФРАСТРУКТУРЕ

F.A.C.C.T.



Профайл

Тип инцидента:

Обнаружена проблема на периметре

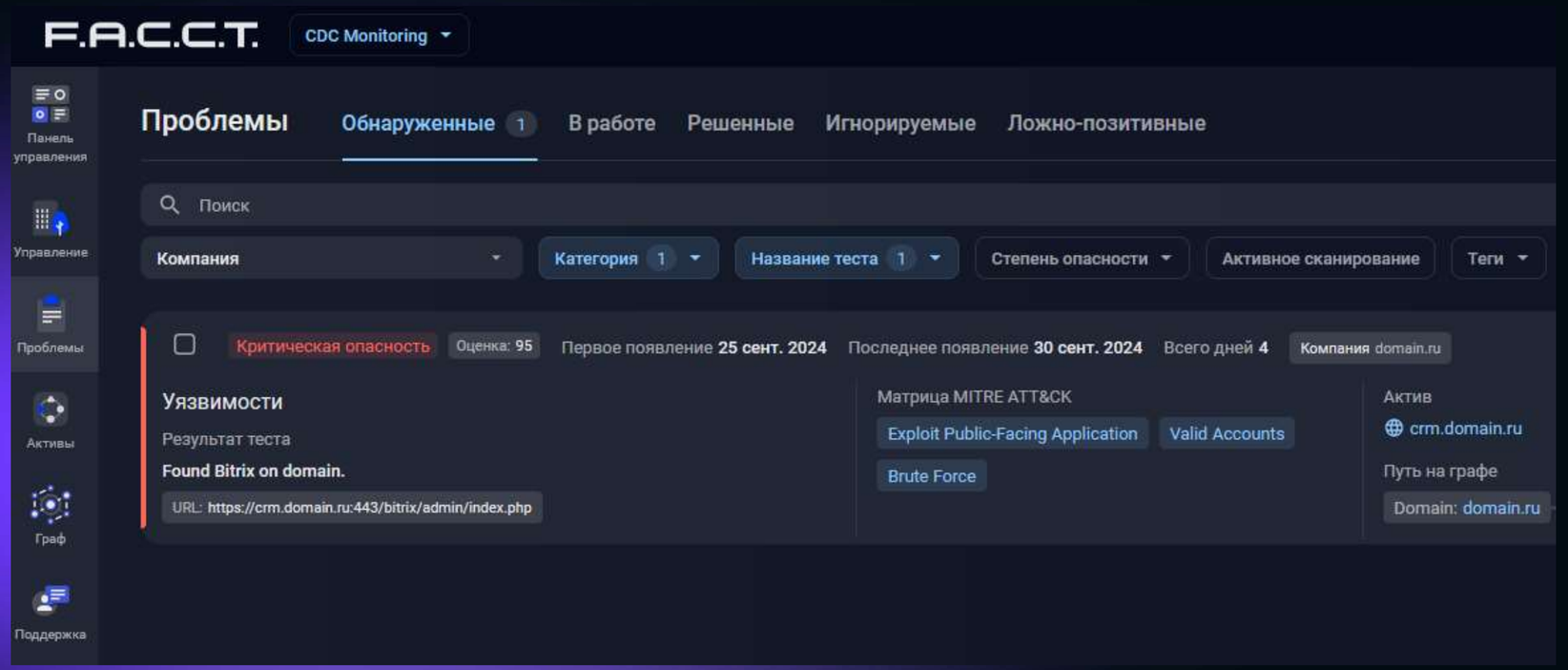
Трендовая уязвимость, которая может быть использована злоумышленниками для получения несанкционированного доступа

Воздействие:

Отсутствует. Следов эксплуатации уязвимостей не обнаружено

ВЫЯВЛЕННЫЕ УЯЗВИМОСТИ

F.A.C.C.T.



Оперативный анализ и реагирование на инцидент

Предоставление рекомендация по сокращению риска:

Обновление Bitrix и его модулей до последней актуальной версии, чтобы закрыть известные уязвимости

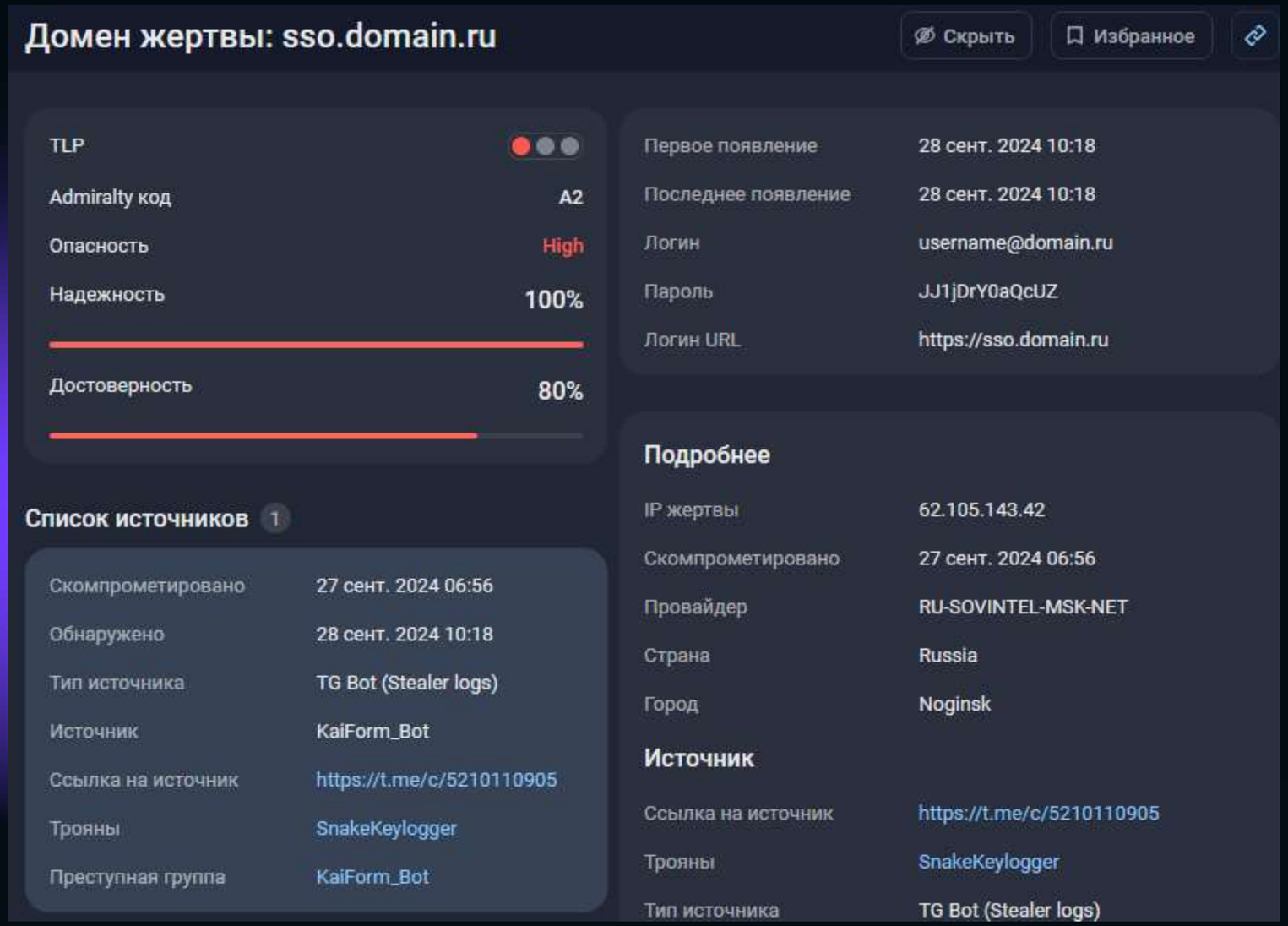
Скрытие логин-формы по стандартному пути, ограничение общего доступа со стороны неавторизованных пользователей

Внедрение MFA

Анализ логов доступа к админ панели, настройка уведомлений о неудачных попытках

ВЫЯВЛЕНЫЕ КОМПРОМЕТАЦИИ УЗ

F.A.C.C.T.



Оперативный анализ и локализация инцидента

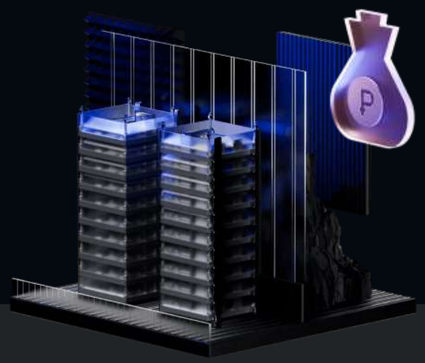
Сбор и исследование данных

Выявление скомпрометированных устройств

Выявление вектора первоначальной компрометации

ВЫВОДЫ

F.A.C.C.T.



Зашифрована

Цифровая криминалистика

Разработка стратегии восстановления

Мероприятия по восстановлению

Выстраивание новой стратегии ИБ

Атака обнаружена и остановлена

Непрерывный мониторинг инфраструктуры

Удаленное реагирование

Изоляция хостов, блокировка вредоносного процесса

Проблема обнаружена и нейтрализована до ее реализации

Непрерывный анализ периметра

Закрытие потенциальных векторов

2-3 месяца простоя

Реагирование и предотвращение

F.A.C.C.T.

Даже в самой худшей судьбе есть возможности для счастливых перемен.
Эразм Роттердамский

F.A.C.C.T.

Технологии для борьбы с киберпреступностью

facct.ru
info@facct.ru

facct.ru/blog
+7 (495) 984 33 64