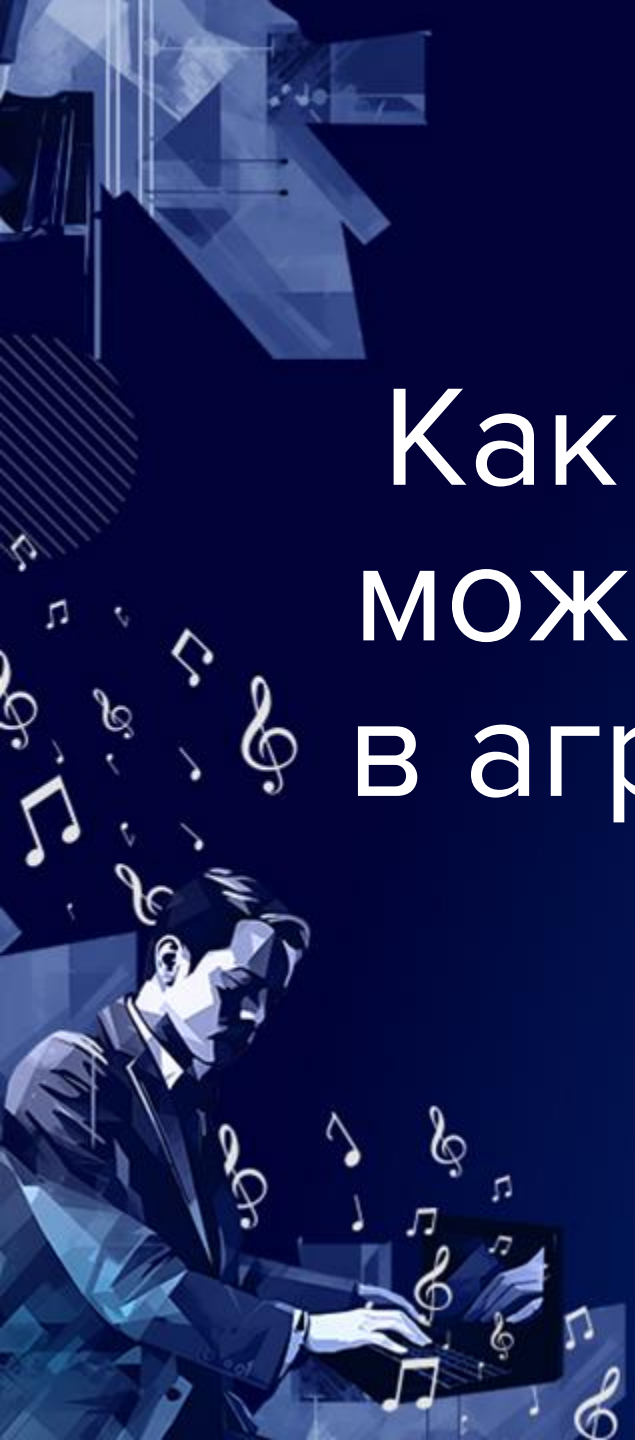
GIS DAYS

# Как искусственный интеллект может побороть естественный в агрессивной среде обитания хакеров

Лукацкий Алексей

Бизнес-консультант по безопасности

Positive Technologies



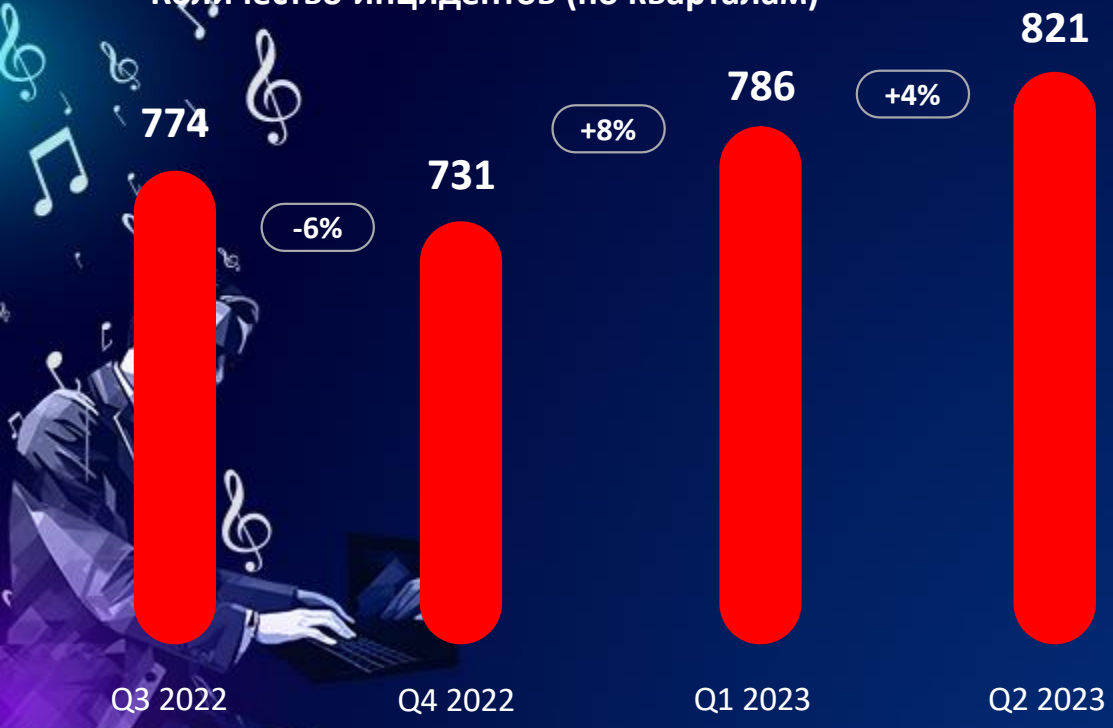
# Число атак все растет: H1 2023

**73%**
Доля целевых атак
(среди всех успешных атак)

**+7%**
Инцидентов относительно
H2 2022 года

**16%**
Доля атак на частных лиц
(среди всех успешных атак)

**Количество инцидентов (по кварталам)**

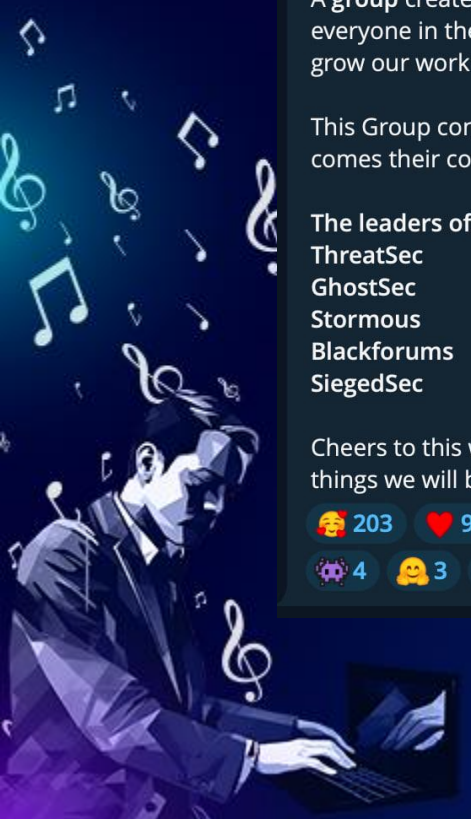



**Категория жертв (ТОП-7)**

# Ключевые наблюдения 2023

- Увеличение времени присутствия в атакованной инфраструктуре
- Атаки через подрядчиков, особенно ИТ/ИБ-компаний
- Снижение числа фейков и компиляций и рост числа реальных утечек
- Маскировка утечек данных под DDoS
- Координация атакующих

# Хакеры объединяют усилия



The Five Families

Now for our major announcement, the creation of a modern day Five Families!

A **group** created to establish better un
everyone in the underground world of
grow our work and operations. We run

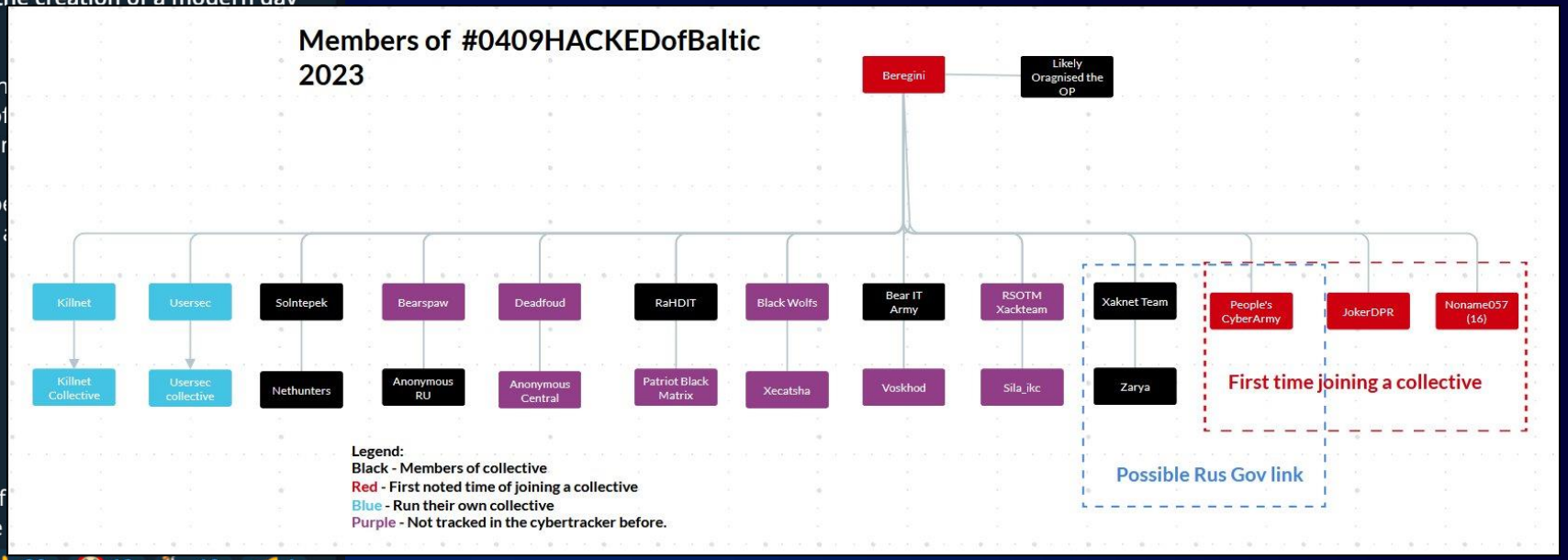
This Group consists and is lead by 5 p
comes their connections, tied groups a

**The leaders of;**
**ThreatSec**
**GhostSec**
**Stormous**
**Blackforums**
**SiegedSec**

Cheers to this wonderful formation of
things we will bring to the table in the

203 96 70 36 29 12 10 4
4 3 1

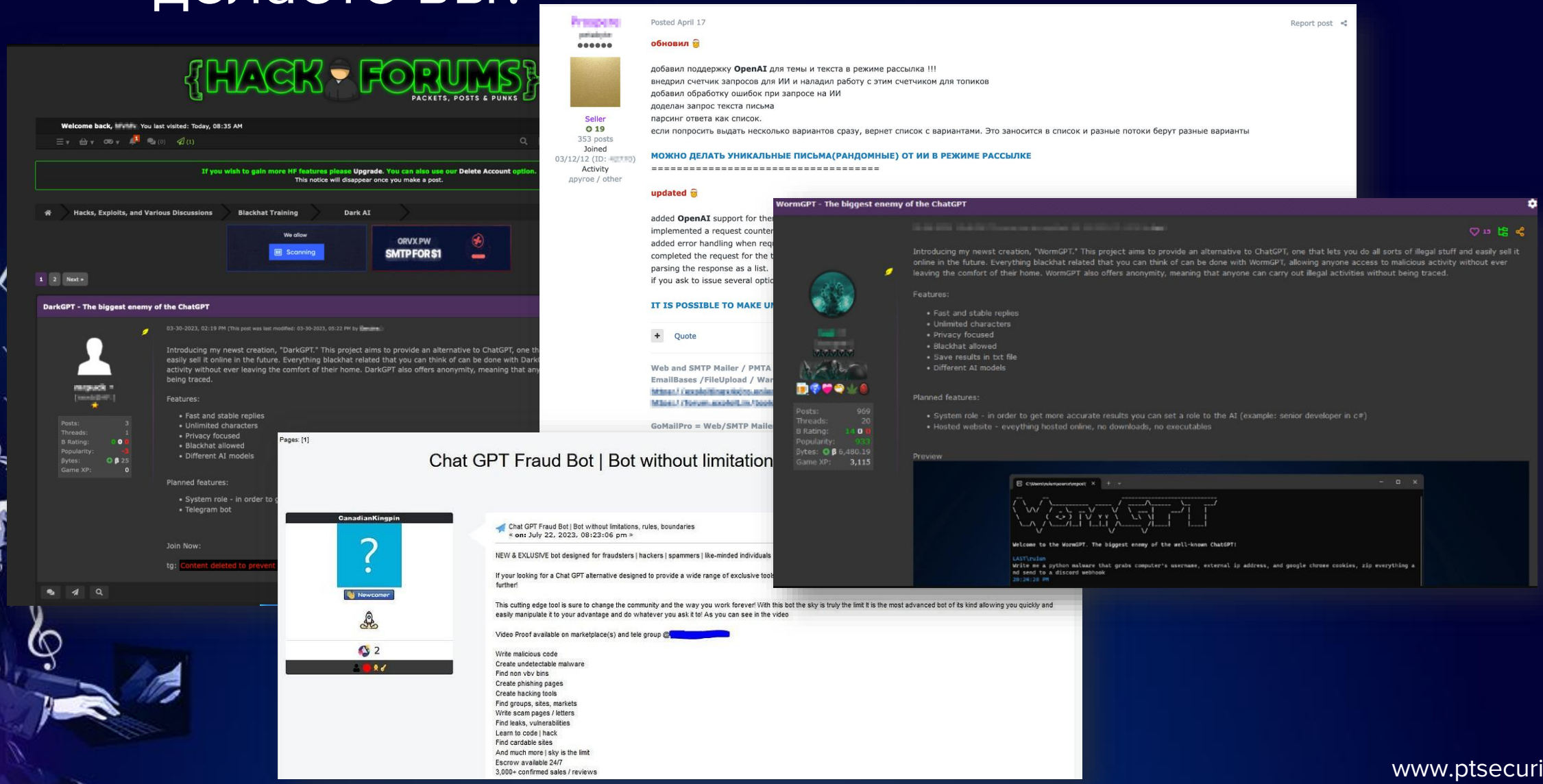
6574 edited 20:10



# А что делать вам?

- Объединение компаний в области ИБ?
  - Конкуренция
- Объединение заказчиков?
  - Утопия
- Внутреннее масштабирование
  - Найм новых сотрудников в ИБ
  - Замена сотрудников роботами

# Если это делают враги, то почему не делаете вы?



# Роботы в ИБ: знать поведение врага

## Изучать врага

Можно не успеть

## Эмулировать врага

Работа на опережение

## Нанимать врага

Если политика позволяет

## Думать как враг

Менять мышление не просто

# Вывод №1: Знание хакеров и их методов

1. Чтобы эффективно бороться с современными хакерами вам нужно иметь собственное подразделение Threat Intelligence с квалифицированным персоналом
2. Если ИБ-компания борется с угрозами (а не занимается, например, СКЗИ или IAM) у нее обязан быть исследовательский центр, а еще лучше, чтобы был и SOC. А иначе откуда им знать про реальные атаки?!

# Киберполигоны

- Разные сценарии / отрасли
- Постоянно действующие или временные
- Синтетический или реальный трафик
- Изучение поведения хакеров и сбор данных о нем

# Данные с киберполигонов = датасет

- Сетевой трафик
- Атаки на приложения
- Разные этапы kill chain
- Цепочки атак
- Поиск Zero Day

# Датасет – это ключ к ИИ в ИБ

## Каков объем и характер?

Чем больше данных для анализа, тем выше эффективность алгоритмов ML

## Есть ли в свободном доступе?

Можете ли вы проверить эффективность приобретаемой или строящейся системы сами? А как сравнивать разные решения?

## Кто и как подготовил?

Чтобы модель ML хорошо сработала, датасет должен быть правильно подготовлен и, в большинстве случаев, размечен

## Пора копить свой датасет

У вас есть преимущество – вы можете собрать данные именно по вашей инфраструктуре. Но вы должны начать и вам нужно хранилище

# Вывод №2: Без датасета вы никто!

1. Полный и регулярно пополняемый датасет – это конкурентное преимущество ИБ-компаний
2. В публичном доступе датасеты по ИБ вряд ли будут появляться в обозримом будущем
3. Возможна генерация синтетических данных, но их применение ограничено

# Модели и алгоритмы ML

- Нет универсального алгоритма для всех задач ИБ. Разные алгоритмы помогают решать разные задачи для разных данных
- Вспоминаем – обучение и исполнение. В процессе исполнения модель не учится! Машинное обучение итеративно и требует регулярного переобучения! «Машинное обучение не требует обновления» – лукавство!
- Выбор алгоритма – это баланс между скоростью работы, аккуратностью предсказания и сложностью модели.
- Исходную задачу можно решить разными способами (алгоритмами). От их выбора зависит точность и скорость решения
- Если датасет неполон или некачественный, то никакой алгоритм не поможет!

# Вывод №3: Знание машинного обучения!

1. Чтобы эффективно применять искусственный интеллект против хакеров вам нужны соответствующие специалисты!
2. ML в движках для обнаружения хакеров, для отработки гипотез, для генерации синтетических данных
3. Если ИБ-компания вам рассказывает про ИИ в ее продуктах, то пусть покажет вам свой отдел по ИИ

# Задавайте правильные вопросы

**Вендору**

1. Какие алгоритмы используются для обнаружения?
2. Какие наборы данных используются в алгоритме
3. Где запускаются алгоритмы (на узле, в ЦОДе, в облаке)?
4. Могут быть алгоритмы обучены на ваших данных?
5. Как много обучающих данных требуется?

**Себе**

1. У вас есть необходимые датасеты?
2. У вас есть квалифицированные аналитики?
3. Какие алгоритмы вы будете использовать?
4. Вы можете использовать open source модели?
5. Как вы будете проверять качество своих моделей?

GIS DAYS

# СПАСИБО ЗА ВНИМАНИЕ

www.ptsecurity.ru