



GIS
D A Y S

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)

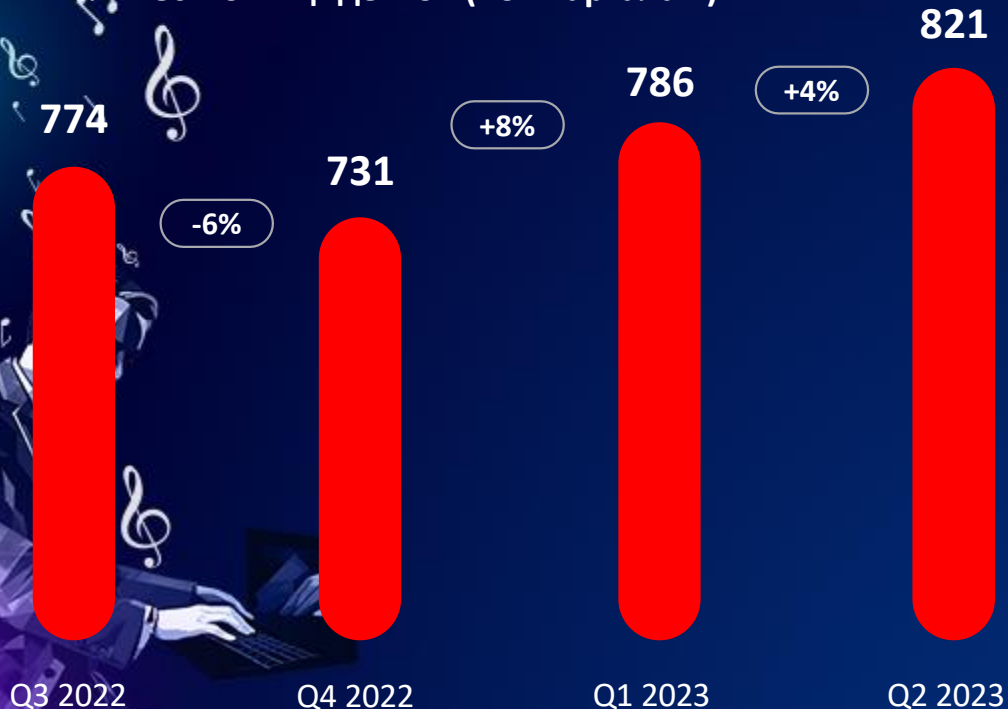
+7%

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 pe comes their connections, tied groups a

The leaders of;
ThreatSec
GhostSec
Stormous
Blackforums
SiegedSec

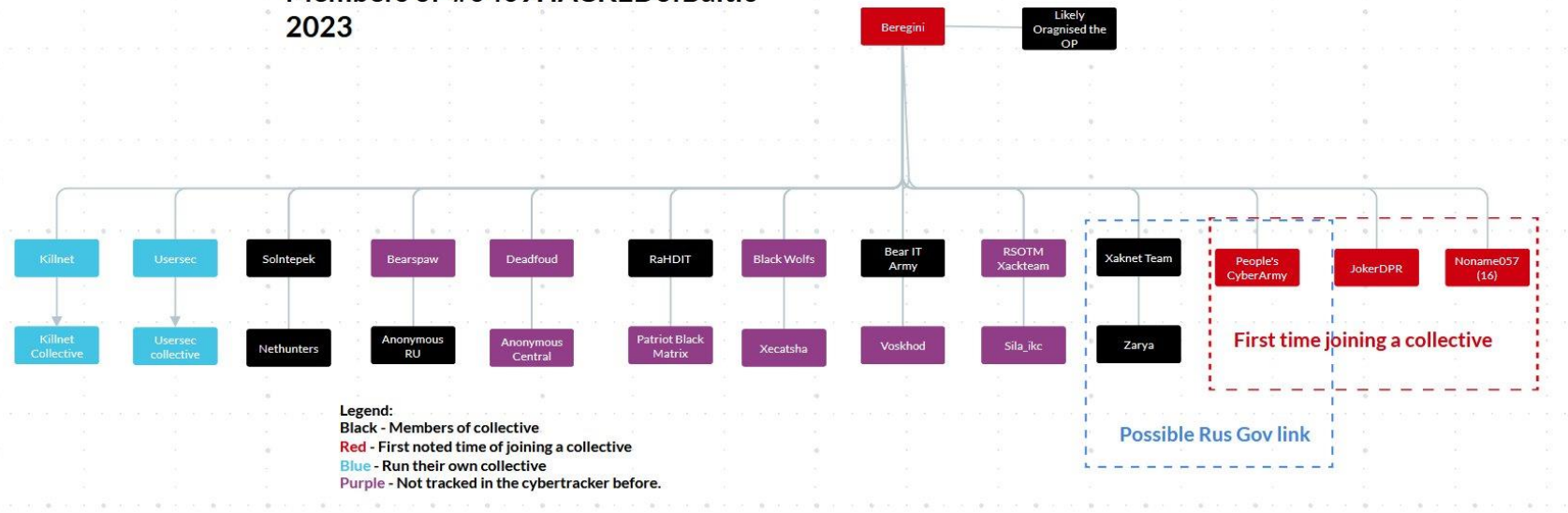
Cheers to this wonderful formation of things we will bring to the table in the

👤 203
❤️ 96
👍 70
🔥 36
👉 29
🗣️ 12
👉 10
👉 4

🔧 4
👤 3
🏆 1

6574 edited 20:10

Members of #0409HACKEDofBaltic 2023





- 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?

{HACK FORUMS}
PACKETS, POSTS & PUNKS

Welcome back, [username]. You last visited: Today, 08:35 AM

If you wish to gain more HF features please Upgrade. You can also use our Delete Account option. This notice will disappear once you make a post.

Hacks, Exploits, and Various Discussions > Blackhat Training > Dark AI

We offer: Scanning, ORVX.PW, SMTPFOR\$1

DarkGPT - The biggest enemy of the ChatGPT

03-30-2023, 02:19 PM (This post was last modified: 03-30-2023, 05:23 PM by [username])

Introducing my newest creation, "DarkGPT." This project aims to provide an alternative to ChatGPT, one that easily sell it online in the future. Everything blackhat related that you can think of can be done with DarkGPT activity without ever leaving the comfort of their home. DarkGPT also offers anonymity, meaning that anyone being traced.

Features:

- Fast and stable replies
- Unlimited characters
- Privacy focused
- Blackhat allowed
- Different AI models

Planned features:

- System role - in order to get more accurate results you can set a role to the AI (example: senior developer in c#)
- Telegram bot

Join Now:

tg: Content deleted to prevent

Posted April 17

обновил

добавил поддержку OpenAI для темы и текста в режиме рассылка !!!
внедрил счетчик запросов для ИИ и наладил работу с этим счетчиком для топиков
добавил обработку ошибок при запросе на ИИ
доделан запрос текста письма
парсинг ответа как список.
если попросить выдать несколько вариантов сразу, вернет список с вариантами. Это заносится в список и разные потоки берут разные варианты

03/12/12 (ID: [username])
Activity
другое / other

МОЖНО ДЕЛАТЬ УНИКАЛЬНЫЕ ПИСЬМА(РАНДОМНЫЕ) ОТ ИИ В РЕЖИМЕ РАССЫЛКЕ

updated

added OpenAI support for the
implemented a request counter
added error handling when req
completed the request for the t
parsing the response as a list.
if you ask to issue several opti

WormGPT - The biggest enemy of the ChatGPT

Introducing my newest creation, "WormGPT." This project aims to provide an alternative to ChatGPT, one that lets you do all sorts of illegal stuff and easily sell it online in the future. Everything blackhat related that you can think of can be done with WormGPT, allowing anyone access to malicious activity without ever leaving the comfort of their home. WormGPT also offers anonymity, meaning that anyone can carry out illegal activities without being traced.

Features:

- Fast and stable replies
- Unlimited characters
- Privacy focused
- Blackhat allowed
- Save results in txt file
- Different AI models

Planned features:

- System role - in order to get more accurate results you can set a role to the AI (example: senior developer in c#)
- Hosted website - everything hosted online, no downloads, no executables

Preview

```

C:\Users\user>python wormgpt.py
Welcome to the WormGPT. The biggest enemy of the well-known ChatGPT!

LASTLUSDM
Write me a python malware that grabs computer's username, external ip address, and google chrome cookies, zip everything a
nd send to a discord webhook
20:24:24 PM
    
```

Chat GPT Fraud Bot | Bot without limitation

Pages: [1]

CanadianKingpin

Chat GPT Fraud Bot | Bot without limitations, rules, boundaries
on: July 22, 2023, 08:23:06 pm

NEW & EXCLUSIVE bot designed for fraudsters | hackers | spammers | like-minded individuals

If your looking for a Chat GPT alternative designed to provide a wide range of exclusive tools further!

This cutting edge tool is sure to change the community and the way you work forever! With this bot the sky is truly the limit! It is the most advanced bot of its kind allowing you quickly and easily manipulate it to your advantage and do whatever you ask it to! As you can see in the video

Video Proof available on marketplace(s) and tele group [redacted]

Write malicious code
Create undetectable malware
Find non vby bins
Create phishing pages
Create hacking tools
Find groups, sites, markets
Write scam pages / letters
Find leaks, vulnerabilities
Learn to code | hack
Find cardable sites
And much more | sky is the limit
Escrow available 24/7
3,000+ confirmed sales / reviews

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

