ANGARA SECURITY

«Взломать любой ценой»

Особенности современных компьютерных атак

Цецерский Артемий

Знакомство

6+
Лет практического опыта в ИБ

60+
Реализованных проектов

1000+
Найденных уязвимостей

- Исследования
- Анализ защищенности
- Эмуляция продвинутых кибератак

Сертифицирован:
- OSCP
- OSEP
- OSWP
- CRTO
- CETP (wip)

Зарегистрированные **CVE** и **BDU**:
Microsoft
Lenovo
Palo Alto
Atlassian
VeraCrypt
InfoTecS
И так далее

Амбассадор киберполигона Standoff

Лучший **хакер** 2025 года в одной из номинаций

Спикер конференций PHDays, ZeroNights, Standoff Talks и т.д.

ИИ делает революцию в ИБ

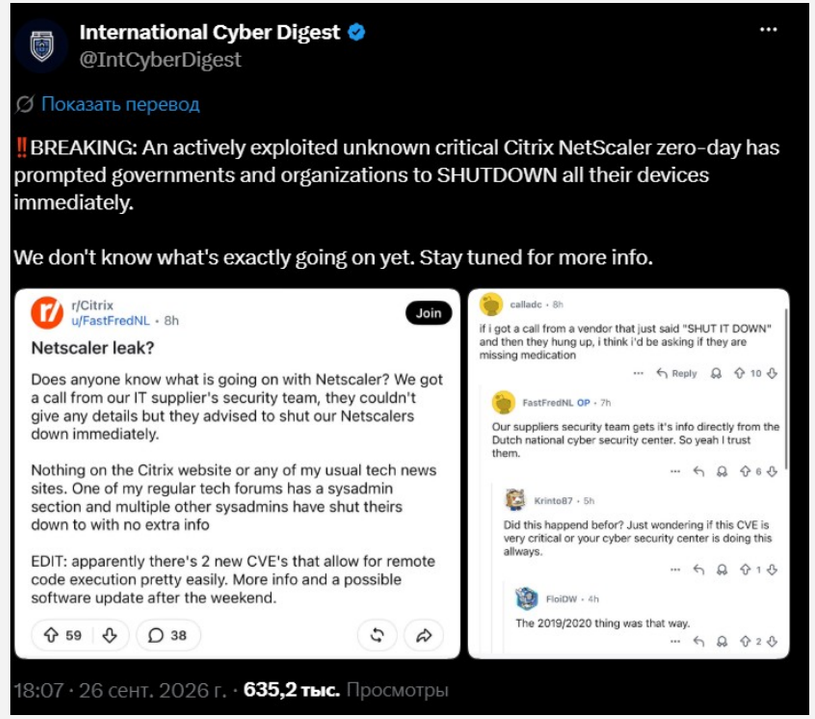
< 24 часов
До получения рабочего эксплойта

+89%
Использование ИИ агентов в атаках

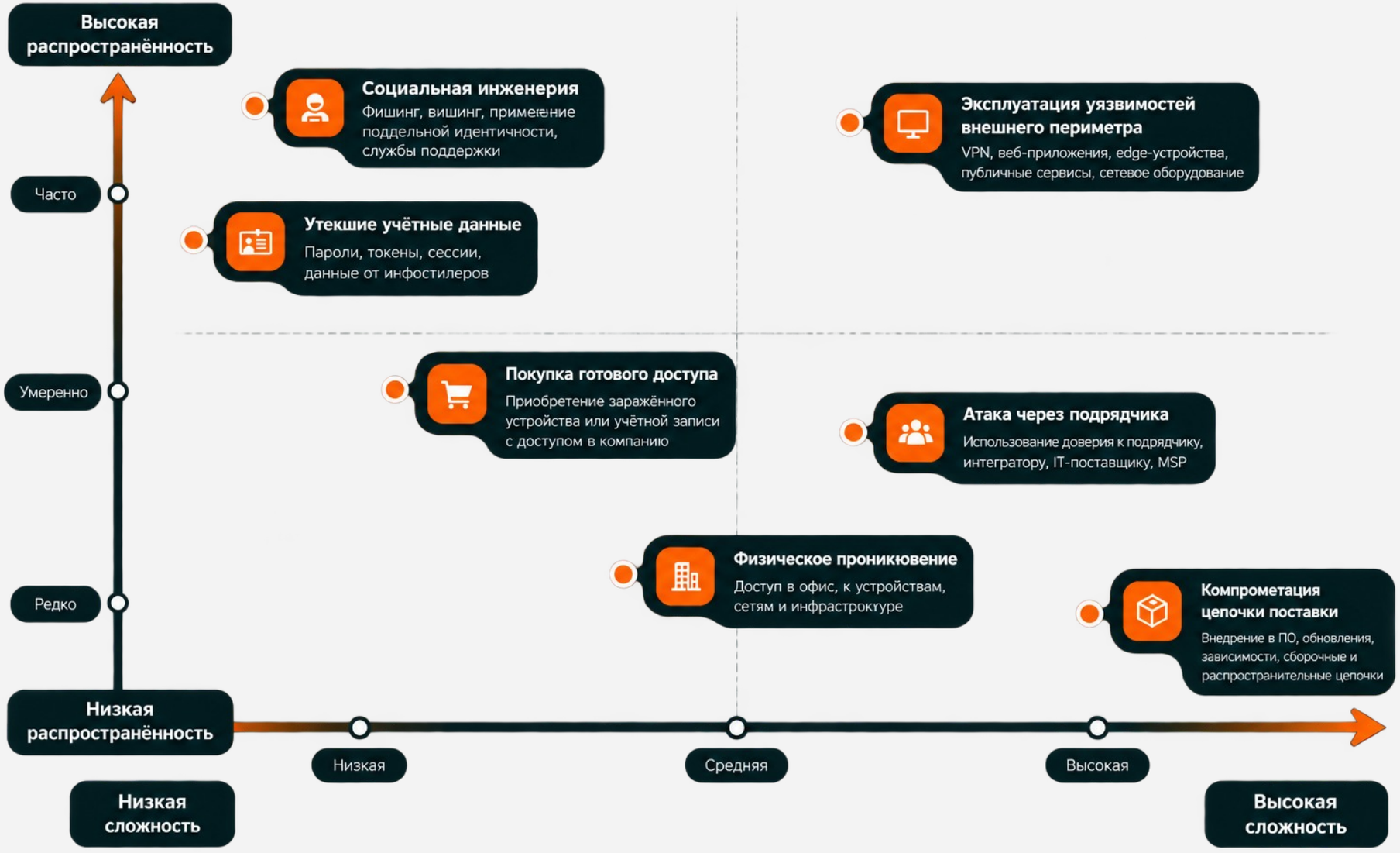
29 минут
Среднее время полной компрометации инфраструктуры

$ 20
Бюджет базовой атаки по цене LLM

- Порог входа
- Стоимость атаки
- Время атаки
- Больше обрабатываемых целей



Актуальные методы проникновения



Массовая атака против целевой

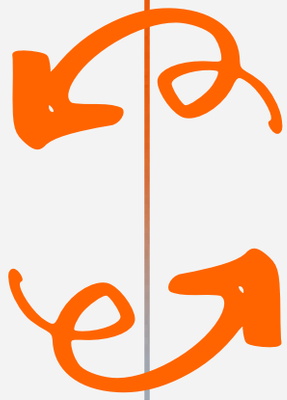
27+
Прогосударственных APT-группировок

8
Новых уникальных

13
Атаковали госучреждения

Массовая атака

- Чаще всего ради финансовой выгоды
- Ботнет
- Майнеры (майнинг криптовалюты)
- Массовый инфостиллер (кража данных)
- Массовая соц.инженерия
- Автоматизированная эксплуатация
- Шифровальщик



Целевая атака

- Взломать любой ценой!
- Тщательная разведка цели
- Знают всю инфраструктуру Покупают уникальное вредоносное ПО или эксплойт под цель
- Точечная проработанная социальная инженерия
- Могут сидеть годами в инфраструктуре

Источник *https://www.f6.ru/resources/research-hub/cybercrime-trends-annual-report-2025-2026/*

Тщательная целевая разведка

Взломать любой ценой. Цена атаки

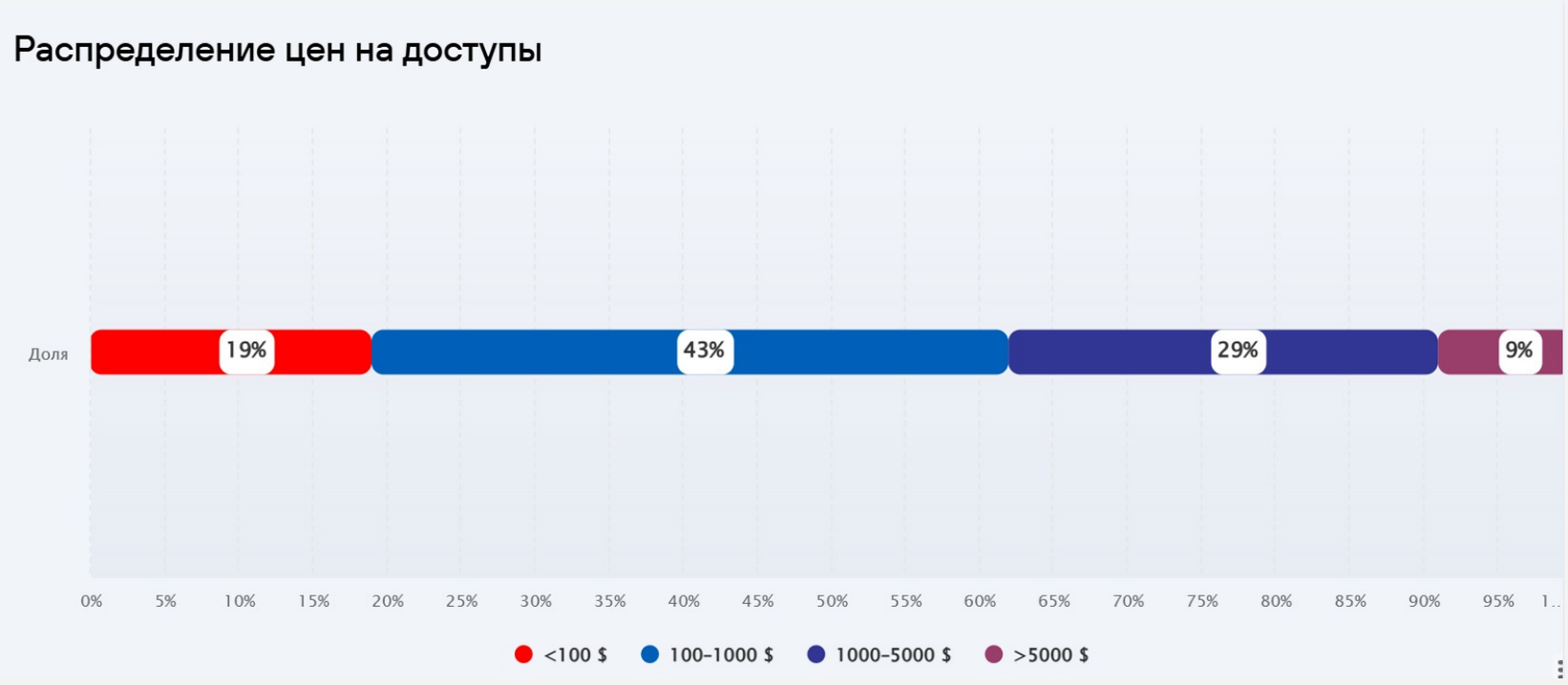
Cybercrime-as-a-Service (CaaS)

61%
Услуг уже готового доступа внутрь

$ 600
Медианная цена корпоративного доступа

$ 27 500
Медианная цена эксплойта

$ 20 млн
Максимальное предложение на рынке за эксклюзивный эксплойт



Источник *https://ptsecurity.com/research/analytics/cybercrime-as-a-service/*

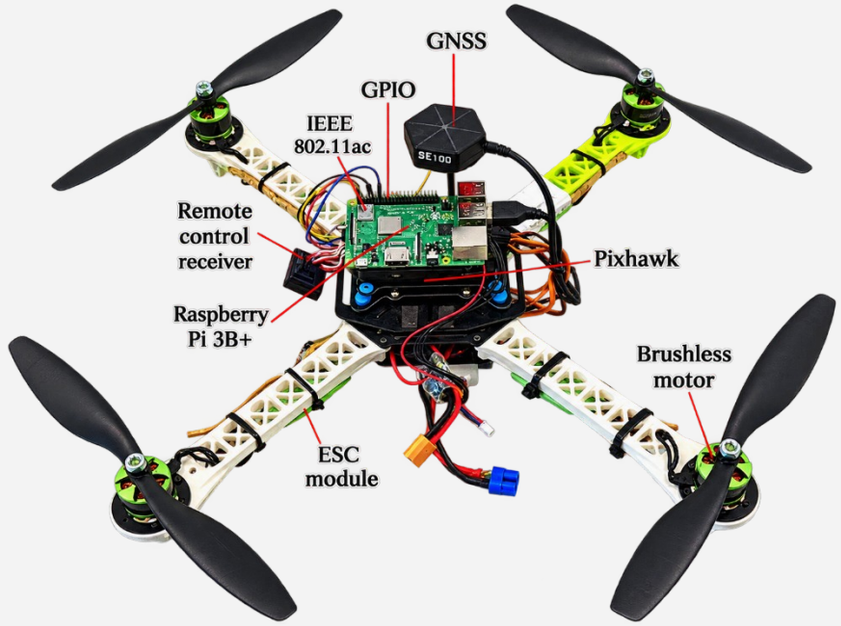
Физическое проникновение в сеть

Обход внешнего периметра защищенного за миллионы рублей

По цене платы за 4000 рублей (Raspberry Pi)

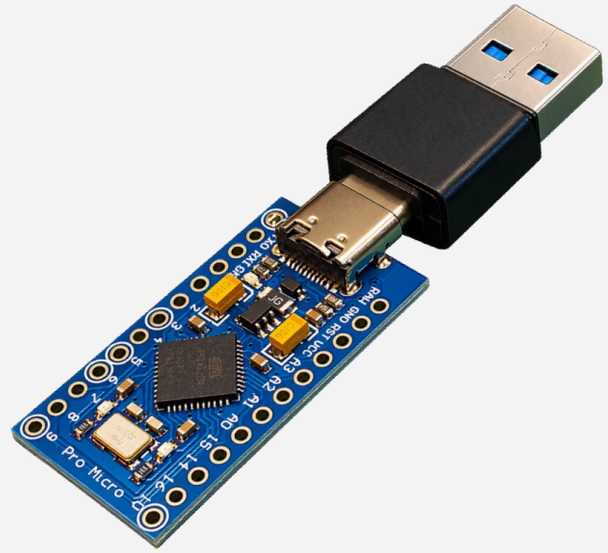
Компрометация беспроводных сетей

В частности с БПЛА



BadUSB / USB HID

USB как устройство ввода с вредоносной нагрузкой



«Мы уже внутри»

27 секунд
Самое быстрое время компрометации инфраструктуры

79%
Реализовывалось критических бизнес-рисков

3.5 часа
Медианное время полной компрометации

- Плоская сетевая инфраструктура (отсутствие сегментирования)
- Небезопасное хранение секретов и паролей
- Недостаточная защита критичных административных сервисов
- Избыточные привилегии
- Старая инфраструктура (Legacy)
- Слабый процесс управления уязвимостями (VM)

Внутренняя часть периметра

Промышленные системы
СУБД
Системы виртуализации
Kubernetes
PKI
FreeIPA
Системы резервного копирования
Облачные технологии
VPN
Active Directory
CI/CD

Источник *https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026*

СЗИ защитит вас от всех бед?

Стереотипное мышление!

48%

Атак выявлялись лишь самой организацией

82%

Атак без классического вредоносного ПО

$ 2150

Медианная цена уникального “убийцы” EDR

Антивирусы или EDR?

Заноза для атакующих, но не абсолютный барьер

Усложняет порог входа атакующих

Межсетевые экраны, фильтрация?

Мимикрия под легитимные корпоративные сервисы: облачные технологии, офисные решения и т.д.

SIEM-системы?

Многие атаки происходят не всегда по паттернам.

Атакующие умеют отключать телеметрию

Время корреляции сотни тысяч событий может быть длительным.

Много событий могут создать лишь шум и лишнее время на обработку

«Песочница» для вредоносного ПО

Сложные многоступенчатые нагрузки

Детектирование среды песочницы

Атака – не всегда сразу вредоносное ПО

Источник *https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-report-findings*

ANGARA SECURITY

Выводы

И при чем тут «эффект бабочки»

Меньше науки, больше практики!

СТАКАН ВОДЫ

Функционально ориентированная цилиндрическая гидродинамическая система временной пространственной локализации, аккумуляции и контролидляруемого перемещения водной жидкой фазы (H_2O) в пределах заданного внутреннего объёмного пространства

Меньше бумаг и регламентов - больше дела

Защищённость определяется не количеством документов, а тем, что произойдёт, когда вас действительно атакуют.

«Благодаря мне, сотрудники Первого Главного Управления КГБ СССР могли работать в Великобритании, как говорится - в полный рост, т.к. работники контрразведки Ми-6 были мной отвлечены на написание никому не нужных бумажных справок и отчетов».

Ким Филби
- заместитель начальника контрразведки,
руководитель 9-го отдела Секретной Разведывательной Службы Великобритании,
советский разведчик, «Почётный сотрудник госбезопасности».

Проверяйте защищенность на практике!

- Тестирование периметра этичными хакерами
- Киберучения (Red Team, Purple Team)

Мониторинг на предмет подозрительной активности

Не только покупайте СЗИ, но и используйте с умом!

Своевременные обновления

Критичные сервисы за VPN

Многофакторная аутентификация

ANGARA SECURITY

Спасибо за внимание!

Контакты

TG: @artemy_ccrsky
Телефон: +7 (926) 381-16-04