tLab

Тренды атак ВПО

Развитие стратегии защиты

Arnur Tokhtabayev (PhD, Founder and R&D)

8 (7172) 57-21-90 info@tntsecure.kz 010000, Astana, Alpamys 17

tLab

Agenda

01 О компании

02 О продукте tLab

03 Тренды

04 Решения

05 Демо

06 Q/A

О компании

Вендор кибербезопасности

- Основана в 2013 году в городе Астана.
- Мотивация – ответ на новые киберугрозы и вызовы в Казахстане и Мире.
- Основатель и генеральный директор имеет многолетний опыт в исследовании и разработке систем в области кибербезопасности в США.
- Целевые клиенты Gov и Enterprise.
- Обширная гос. поддержка (Astana Hub, НАТР, Реестр доверенного ПО)

Тренды в атаках на промышленность

Целевые атаки на промышленность

Пример: В 2021-2022 годах произошло несколько атак на промышленные системы, с нарушения работы нескольких заводов и энергетических компаний

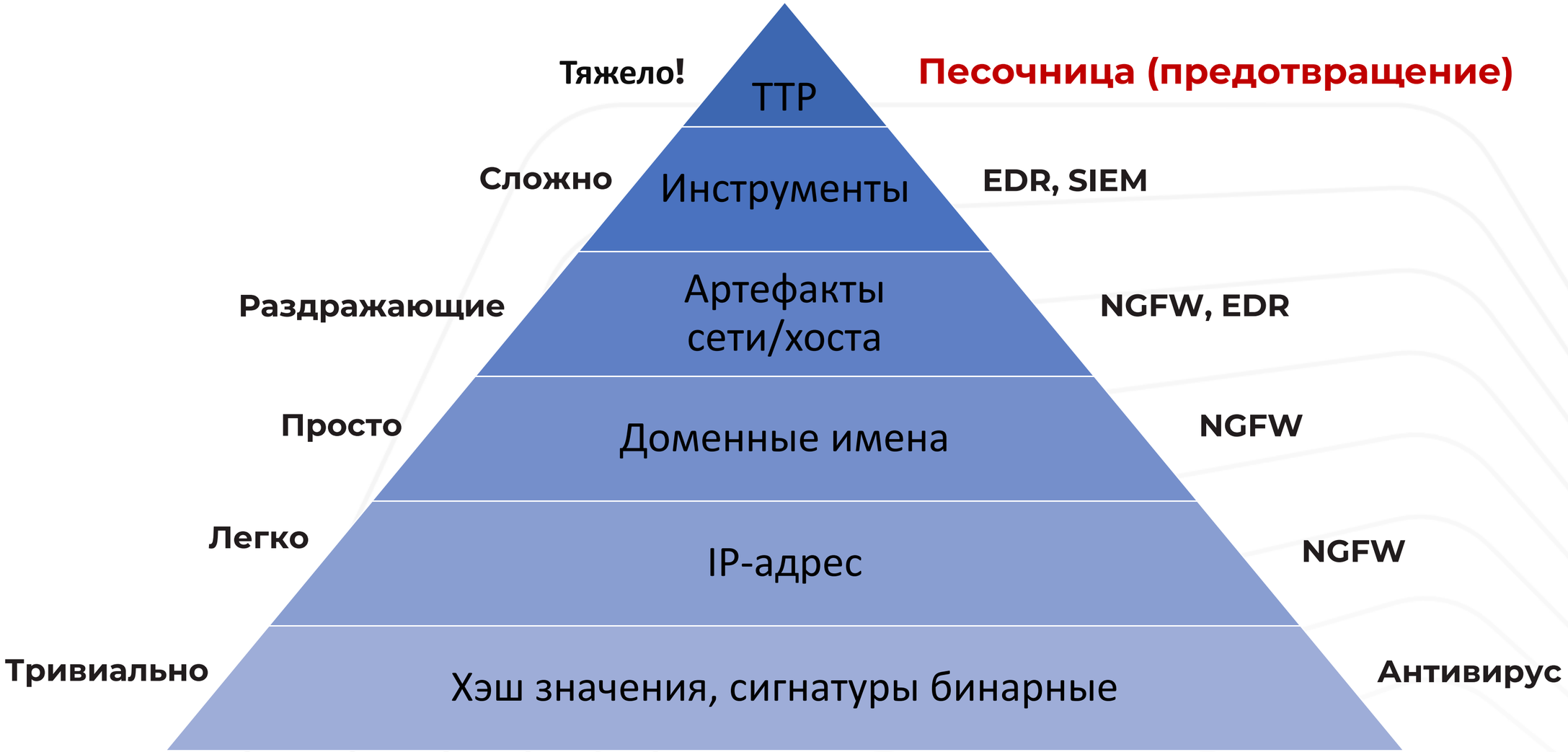
Кейс: Атака на компанию Colonial Pipeline в 2021 году привела к временной остановке одного из крупнейших трубопроводов в США, что вызвало дефицит топлива и панику среди населения

Рост сложности атак

Пример: Pipedream – новое вредоносное ПО, нацеленное на системы управления промышленными объектами (ICS/OT), разработанное, по мнению экспертов, государственным актором для возможных будущих деструктивных операций.

Угроза: Атака на заводы и распределительные сети с использованием такого ПО может привести к катастрофическим последствиям для производства и безопасности населения.

"Пирамида боли”
Сложность обхода защиты



Эффективная защита

от современных целевых, APT и ВПО нулевого дня

tLab Anti-APT

- **DeepTech в кибербезопасности**

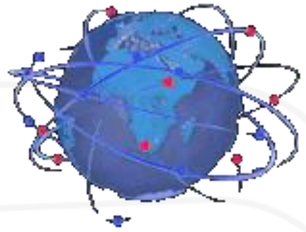
  10+ публикаций в США и Европе, 120 цитат

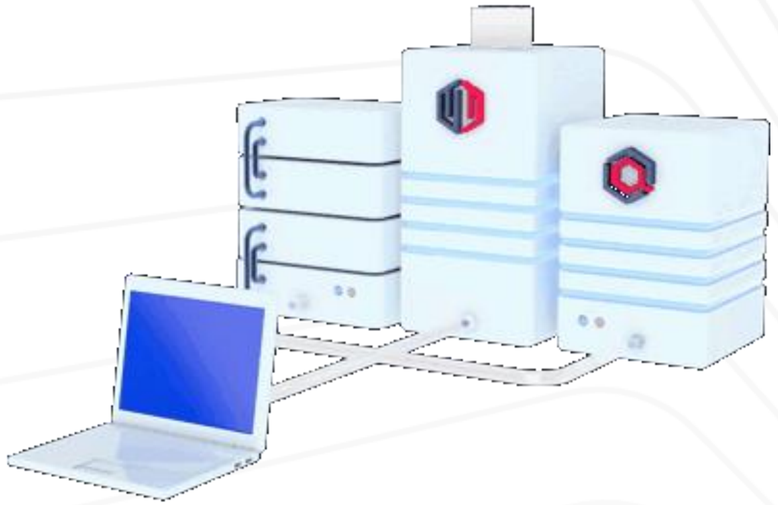
- **tLab доверяют мировые вендоры**

  Соглашение о взаимодействии с Trend Micro и Check Point (интеграция решений)

- **tLab внедрен**

  Парламент РК, Киберщит РК, Национальный банк, ОЦИБ (ЦЭФ, ЦРТР, МИИР и др)

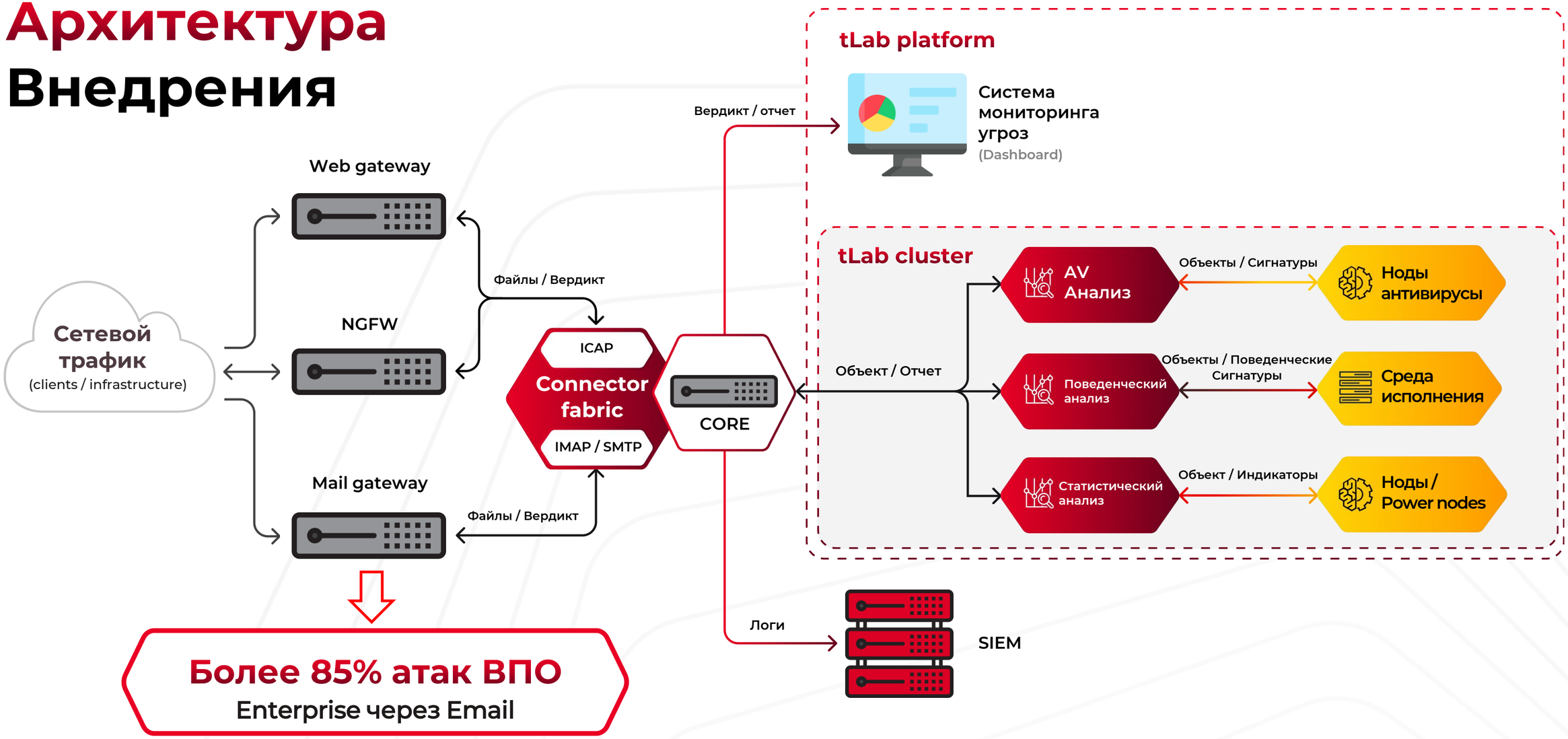




Более 10 миллионов файлов

Проанализированы в различных организациях РК

Архитектура Внедрения



VirLab

Работает на опережение

Как злоумышленники работают? Какую цель они преследуют?

Вирусные аналитики занимаются поиском вредоносных файлов и атак нового типа. Производится детальный мониторинг объектов по различным критериям, в числе которых: регион, ключевые слова и другие.

Reverse-engineering: разбор объекта на "атомы"

Вирусные аналитики выполняют глубокий ручной анализ объекта. Более того, в исследовании специалисты опираются на результат динамического анализа в системе «tLab».

Первичный отчет в период от 1 до 3 дней (IOCs, YARA, полный отчет)

Если вредоносное ПО обладает обширным функционалом, создается подробный отчет с описанием работы объекта и результатом сканирования «tLab». Параллельно формируются Yara-правила

Приложение 1 Индикаторы компрометации

Индикатор компрометации (IOC)	Значение/hash (sha256)	Описание
Домены (URL)		
https://ventusdistribucija[.]hr https://ventusdistribucija[.]hr / MiG31.jpg	https://ventusdistribucija[.]hr	Download server - сервер загрузки вредоносного скрипта (). Статус (24.08.2022): Web-сайт - доступен Объект (MiG31.jpg) - недоступен.
ftp.akmokykla[.]lt	ftp.akmokykla[.]lt	C2C сервер Agent Tesla (отправка данных)
Объекты/файлы		
Келісімшарттық құжаттама.chm	e5f8e155895cd516ffa5102813d667613ceebcc10ca91ea2c1abb94c539caad4	Downloader - скомпилированный HTML-файла полученный по почте
MiG31.jpg	516dad3fe191f821a44dd81fc8b726849fac2a15d7e1b585189d801a322285d3	Dropper - PowerShell-скрипт (скачиваемый с сервера загрузки)
Sneaky DLL	3c4a9a01a27397525f7e8a70b025d5e77951c90efdf02b3ca979432b344d3c0e	.NET Injector – DLL для инъекции вредоносного исполняемого файла в легитимный процесс (метод – Process Hollowing)
Agent Tesla	06c26459844cc452ae5a9ff7e493723691bddd625d45d02c5452bd3a38d28cdd	Trojan-Stealer – вариация трояна с шпионским функционалом Agent Tesla

Таблица 1 Индикаторы компрометации (IoC)

Анализ сложных мировых угроз

Фокус на казахстанские кейсы

Реагирование в течении одного дня

От получения угрозы до отчета (Yara-правило)

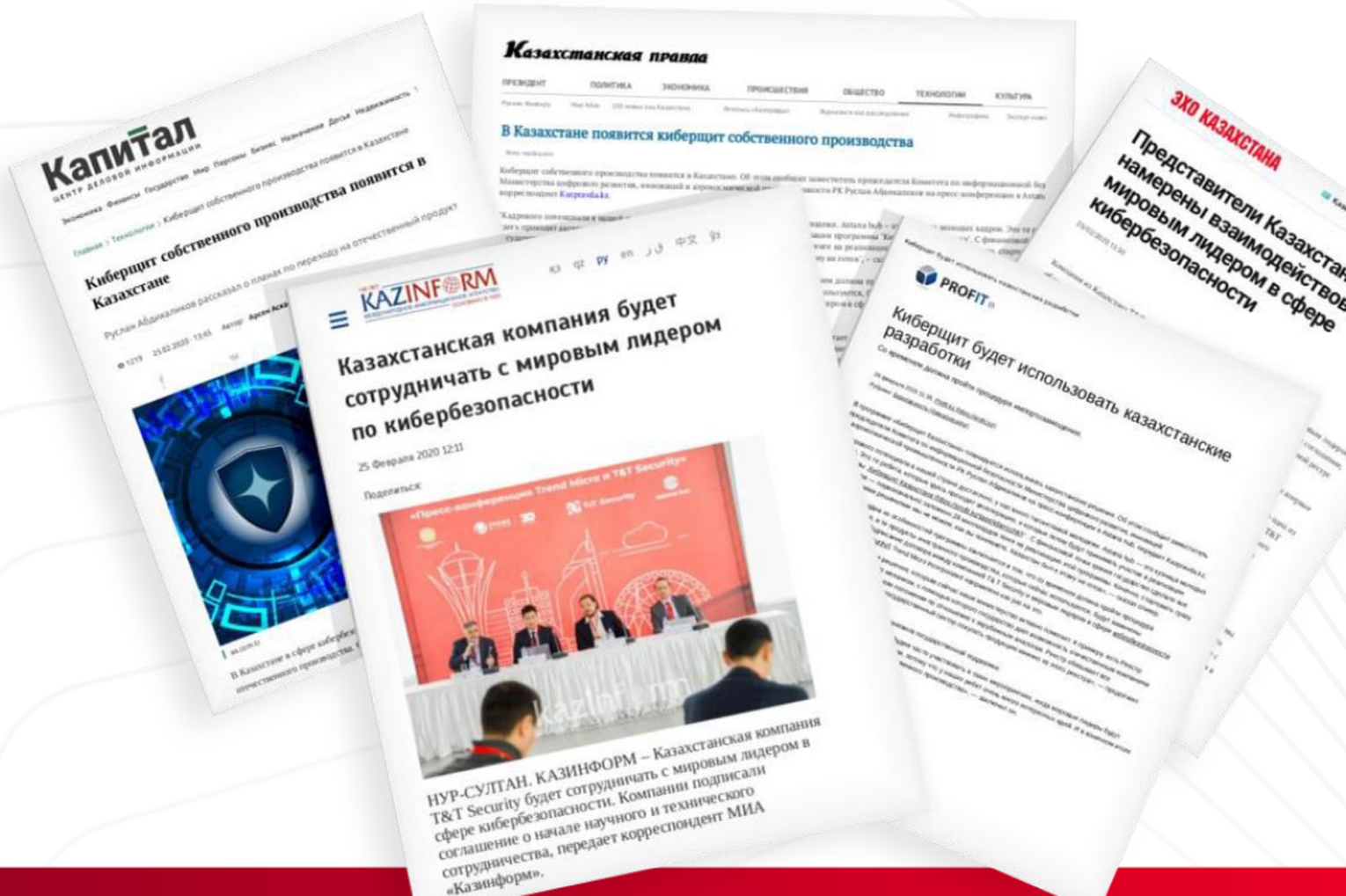
Успешное Сотрудничество

Партнерство с мировым лидером TrendMicro

Научно-техническое сотрудничество

Интеграция tLab с решениями от TrendMicro

Комплексное совместное решение



Кейсы: обнаружение ВПО в tLab и анализ в VirLab (с начала 2024)

- **Infostealer (шпионское ПО)**

  Детект: Обнаружено в 2 организациях

  Угроза: Кража учеток от более 40 приложений и сайтов

  Анализ: отчеты, IoC, YARA-сигнатуры, исследование

- **RAT (удаленный доступ)**

  Детект: Обнаружено в 1 организации

  Угроза: Удаленный доступ, скриншоты и запись аудио

  Анализ: отчеты, IoC, YARA-сигнатуры

- **Reconnaissance (сканер сети и разведка)**

  Детект: Обнаружено в 1 организации

  Угроза: Сканирование сети, поиск уязвимостей и их эксплуатация

  Анализ: отчеты, сложная обфускация

Q/A Session