Advanced Technologies Solutions

нePENtest

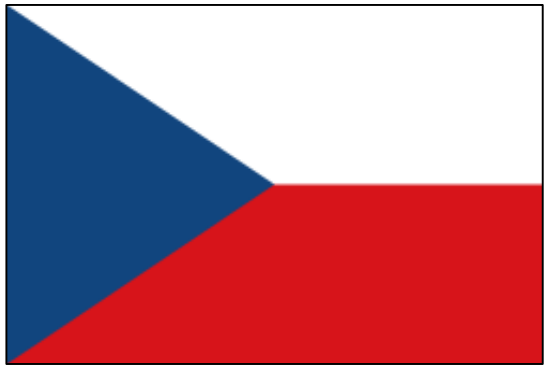
COMPROMISE ASSESSMENT

Выявление следов компрометации и признаков подготовки хакерской атаки

Aleksandr Tvaradze

Advanced Technologies Solutions

Азербайджан



Чехия

Сербия

Украина

Россия

Advanced Technologies Solutions

ISSP

nccgroup

EKRAN

INFOWATCH

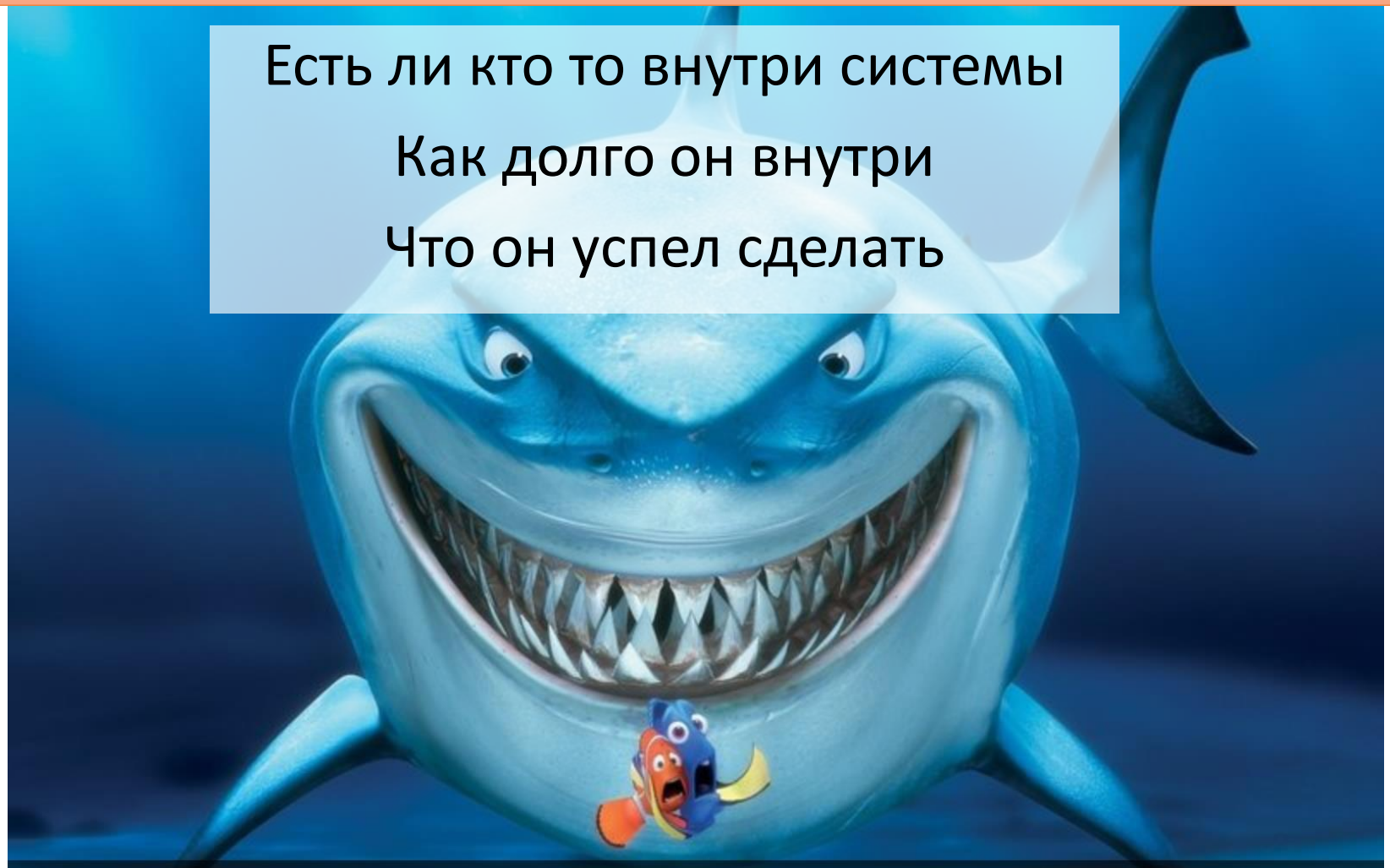
ivanti

ПРОДУКТЫ И СЕРВИСЫ

- Информационная безопасность
- Решения для физической безопасности
- Аудит в области ИТ и ИТ-безопасности
- Онлайн сервисы
- FinTech

Как понять что вы все еще в безопасности?

Взломан или не взломан – вот в чем вопрос



Есть ли кто то внутри системы

Как долго он внутри

Что он успел сделать

Advanced Technologies Solutions

Что нам дает PEN Тест ?

- Моментальный слепок уязвимостей на момент тестирования
- Список уязвимостей на момент PEN теста
- Можно ли нас взломать на момент PEN теста

PEN Тест никак не отвечает на эти вопросы

- Есть ли кто то внутри системы
- Как долго он внутри
- Что он успел сделать

Advanced Technologies Solutions

Как долго длится взлом?

Атакующие являются резидентами внутри систем

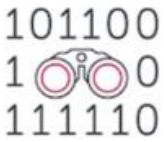
От 160 до 469 дней до обнаружения

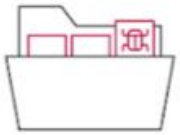
40 дней от проникновения в сеть до вывода $2 млн
в 2016 году один из крупнейших банков Тайваня — **First Bank**, был ограблен на **2 млн долларов**.
Атаку осуществила группировка Cobalt.
С момента **заражения** до вывода денег прошло **40 дней**, все это время действия злоумышленников оставались незамеченными для службы безопасности банка.

Advanced Technologies Solutions

из отчета Group-IB

Фазы атаки





Разведка | Экипировка | Вторжение | Исследование | Маскировка | Спящий агент | Достижение целей | Зачистка

Цель Compromise Assessment

- Найти следы подготовки к хакерской атаке
- Найти признаки компрометации данных
- Оценить масштаб ущерба и выяснить - какие системы были атакованы.

КАК ЭТО ПРОИЗОШЛО

Используются методы атак которые не известны системам безопасности

Используются легальные системы и продукты

Взлом происходит через доверенные подключения, подрядчиков или партнеров

Advanced Technologies Solutions

ЧТО АНАЛИЗИРУЕМ

- Журналы ПК и Серверов
- Сетевые журналы
- Временные файлы
- Дамп памяти при необходимости

Определение IoC и поведенческих аномалий

ДЕЙСТВИЯ

- Определение показателей, возможной компрометации внутренней инфраструктуры хакерами.
- Выявление потенциальных нарушений в соответствии с практиками информационной безопасности.
- Предоставление аудиторских доказательств:
  - обнаруженные показатели;
  - ранжирование по степени риска;
  - Рекомендации по смягчению последствий.

Blood Test Results Report

The Blood Test Results Report lists the results of the patient's Chemistry Screen and CBC and shows you whether or not an individual element is outside of the optimal range and/or outside of the clinical lab range. The elements appear in the order in which they appear on the lab test form.

Above Optimal Range	Above Standard Range	Alarm High
14 Current 9 Previous	4 Current 8 Previous	0 Current 1 Previous

Below Optimal Range	Below Standard Range	Alarm Low
9 Current 0 Previous	0 Current 0 Previous	0 Current 0 Previous

Element	Current Jun 14	Previous Jan 27	Impr	Optimal Range	Standard Range	Units
Glucose	89.00 ↑	91.00 ↑			65.00 - 99.00	mg/dL
Hemoglobin A1C	5.40	5.50			0.00 - 5.70	%
Insulin - Fasting	6.80 ↑	2.00			0.00 - 23.00	µIU/ml
BUN	12.00	11.00			7.00 - 25.00	mg/dL
Creatinine	0.81	0.83			0.50 - 1.05	mg/dL
BUN/Creatinine Ratio	15.00	13.25			6.00 - 22.00	Ratio
PSA	0.60	0.60			0.00 - 4.00	ng/ml
eGFR Non-Afr. American	96.30	95.20			60.00 - 128.00	/min/1.73r
Sodium	140.00	140.00			135.00 - 146.00	mEq/L
Potassium	4.40	4.10			3.50 - 5.30	mEq/L
Sodium/Potassium Ratio	31.82	34.15			30.00 - 35.00	ratio
Chloride	104.00	100.00			98.00 - 110.00	mEq/L
CO2	25.00	26.00			19.00 - 30.00	mEq/L
Anion gap	15.40 ↑	18.10 ↑↑			6.00 - 16.00	mEq/L
Uric Acid, male	4.30	4.10			4.00 - 8.00	mg/dL
Protein, total	7.10	7.70 ↑			6.10 - 8.10	g/dL
Albumin	4.50	5.00			3.60 - 5.10	g/dL
Globulin, total	2.60	2.70			1.90 - 3.70	g/dL

Анали «крови» ИТ структуры

Advanced Technologies Solutions

ЭТАПЫ

Advanced Technologies Solutions

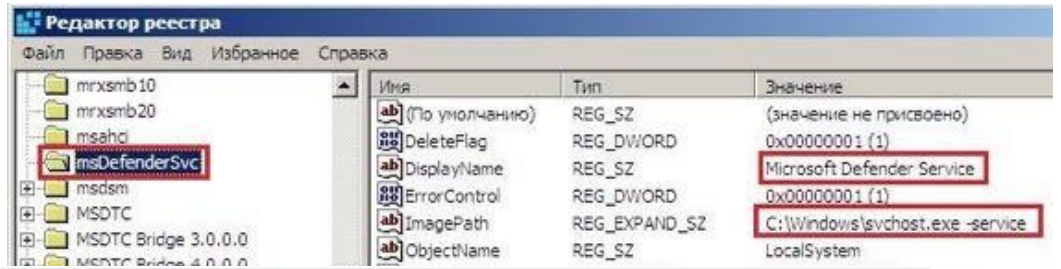
Сбор логов

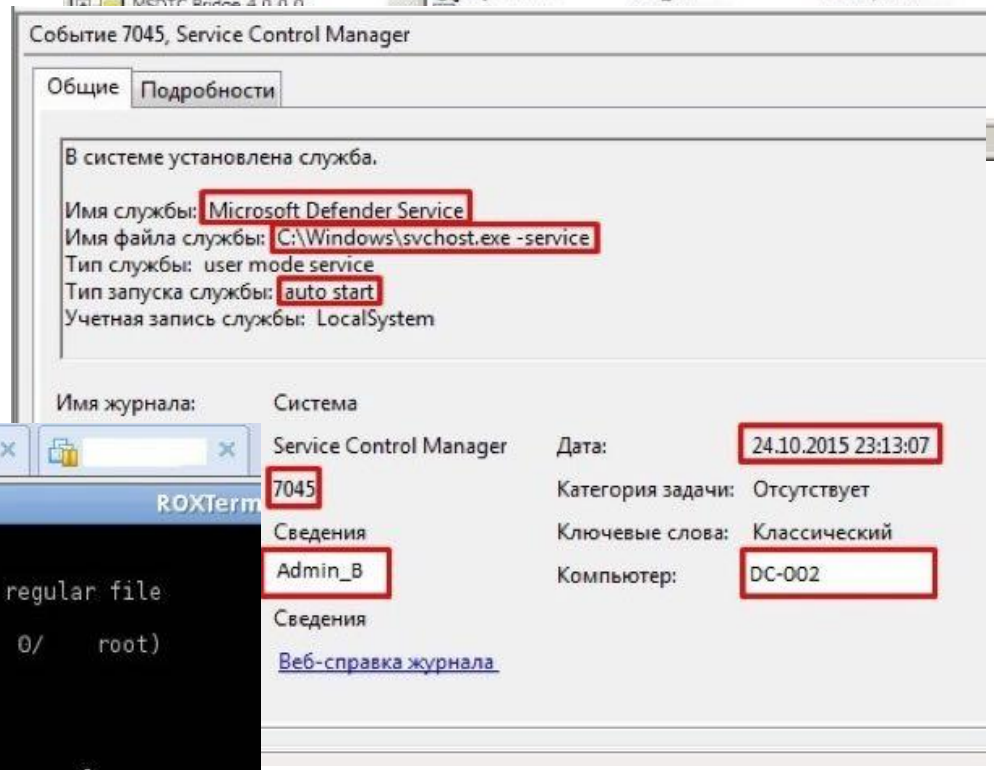
Дополнительная информация

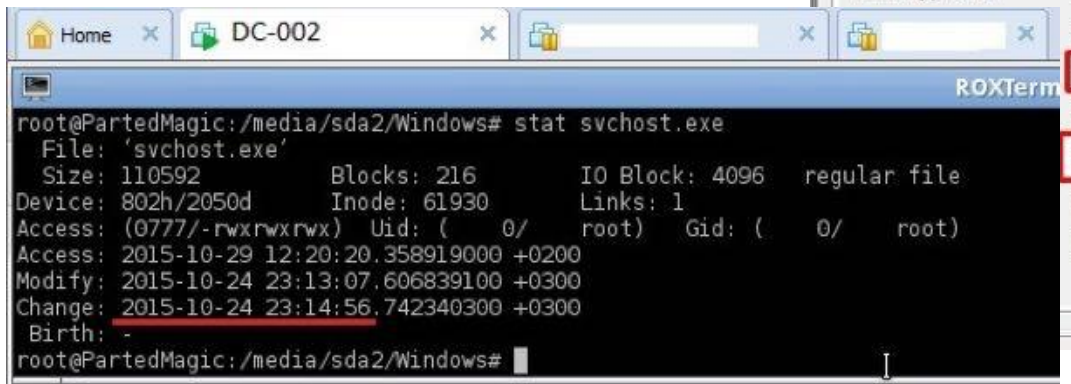
Анализ

Отчет

- Сбор логов с серверов и рабочих станций
- Запуск скриптов – быстро и безопасно
- Тип собираемых логов
- **System, Security, Application, OAlerts**







Advanced Technologies Solutions

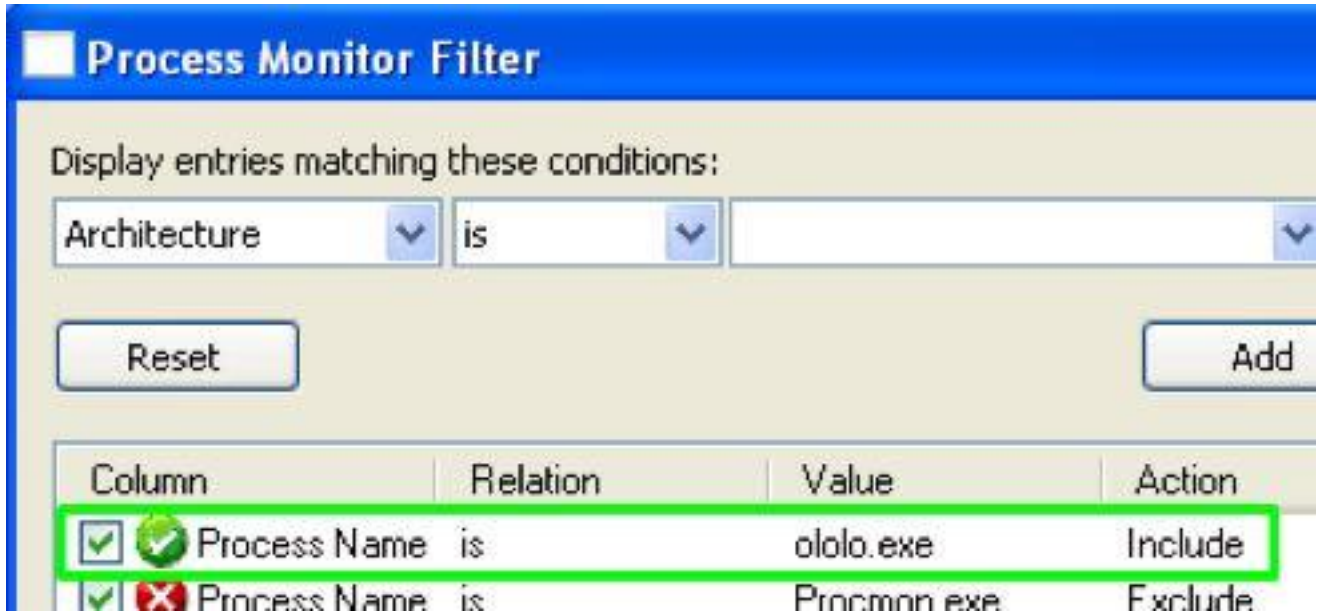
Сбор логов

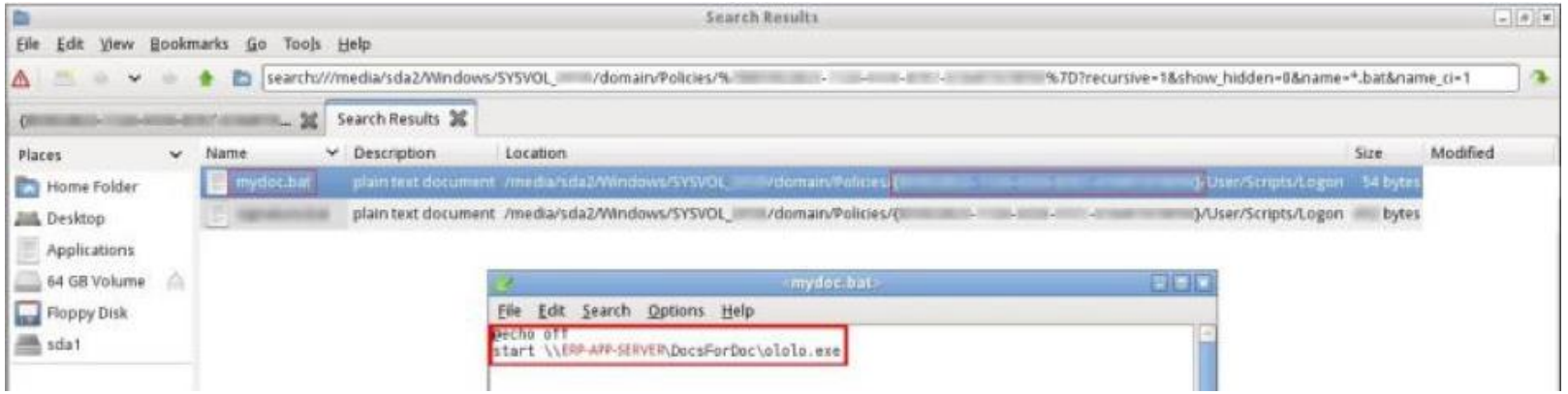
Дополнительная информация

Анализ

Отчет

- Сбор папок и файлов **C: \ Windows \ System32 \ drivers **
- Сбор файлов из временных папок
- Сбор информации из AD

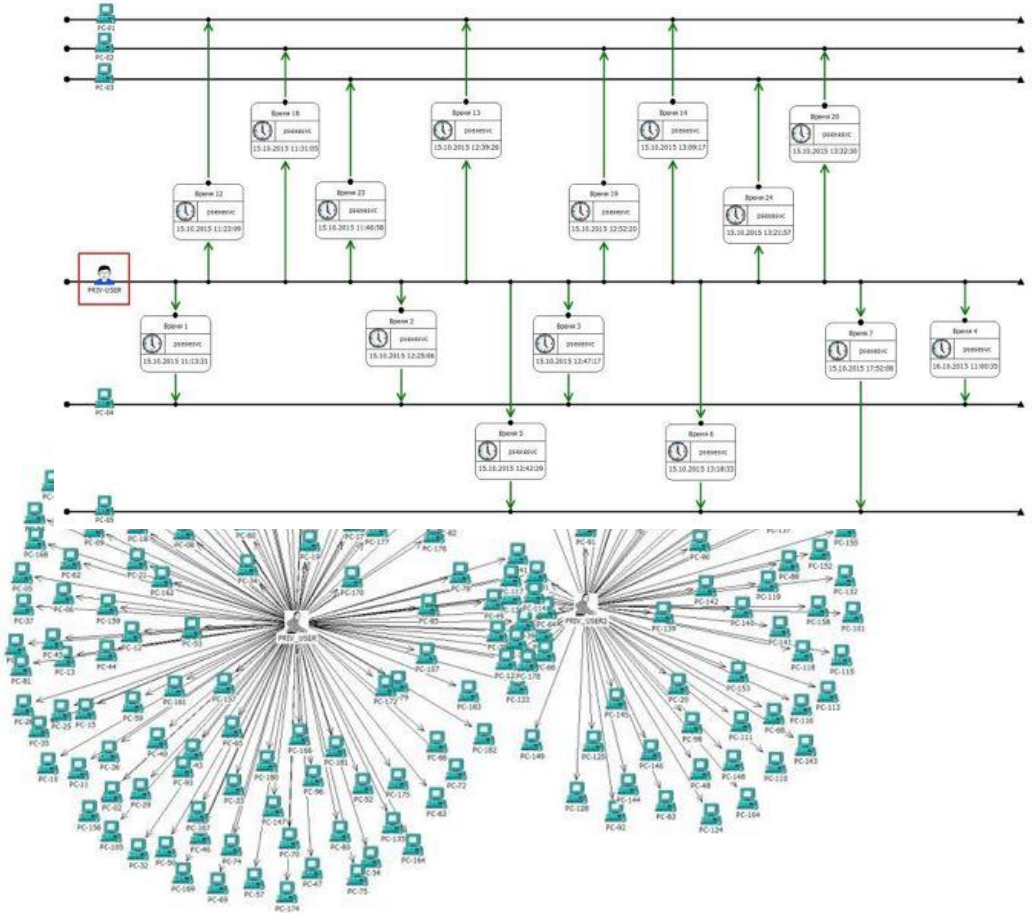




Advanced Technologies Solutions

Сбор логов | Дополнительная информация | **Анализ** | Отчет

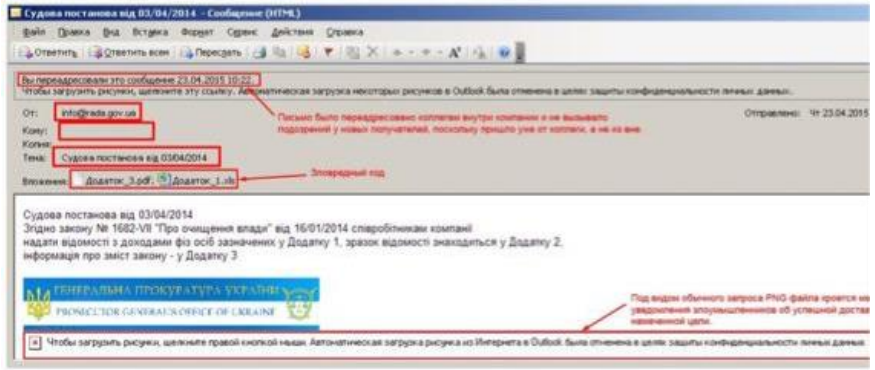
- Проверка целостности полученных логов и артефактов
- Анализ данных и анализ артефактов путем
- Выявления аномалий поведения
- Ручной анализ
- Моделирование потенциальных кибератак
- Визуализация результатов
- Получение IoC

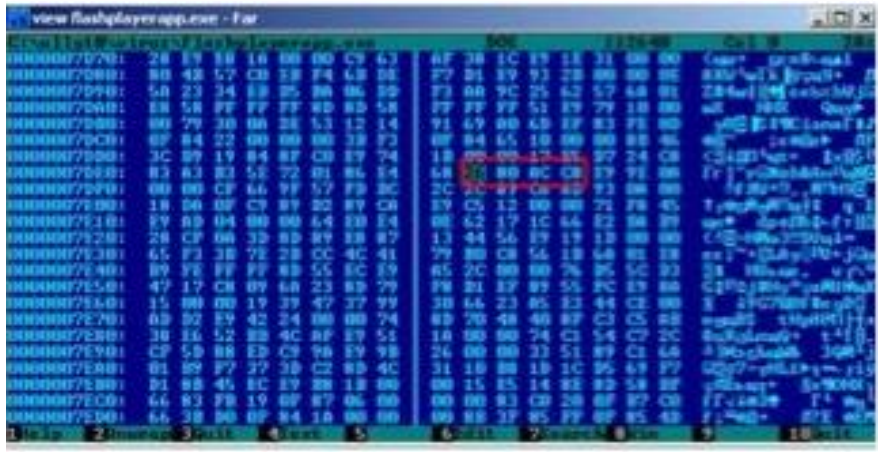


Advanced Technologies Solutions

Сбор логов → Дополнительная информация → Анализ → **Отчет**

- Статус компрометации инфраструктуры
- Список показателей IoC
- Обнаруженных аномалии поведения сервисов, пользователей и программного обеспечения
- Reverse engineering для вредоносного ПО
- Подробные рекомендации по дальнейшему внутреннему расследованию

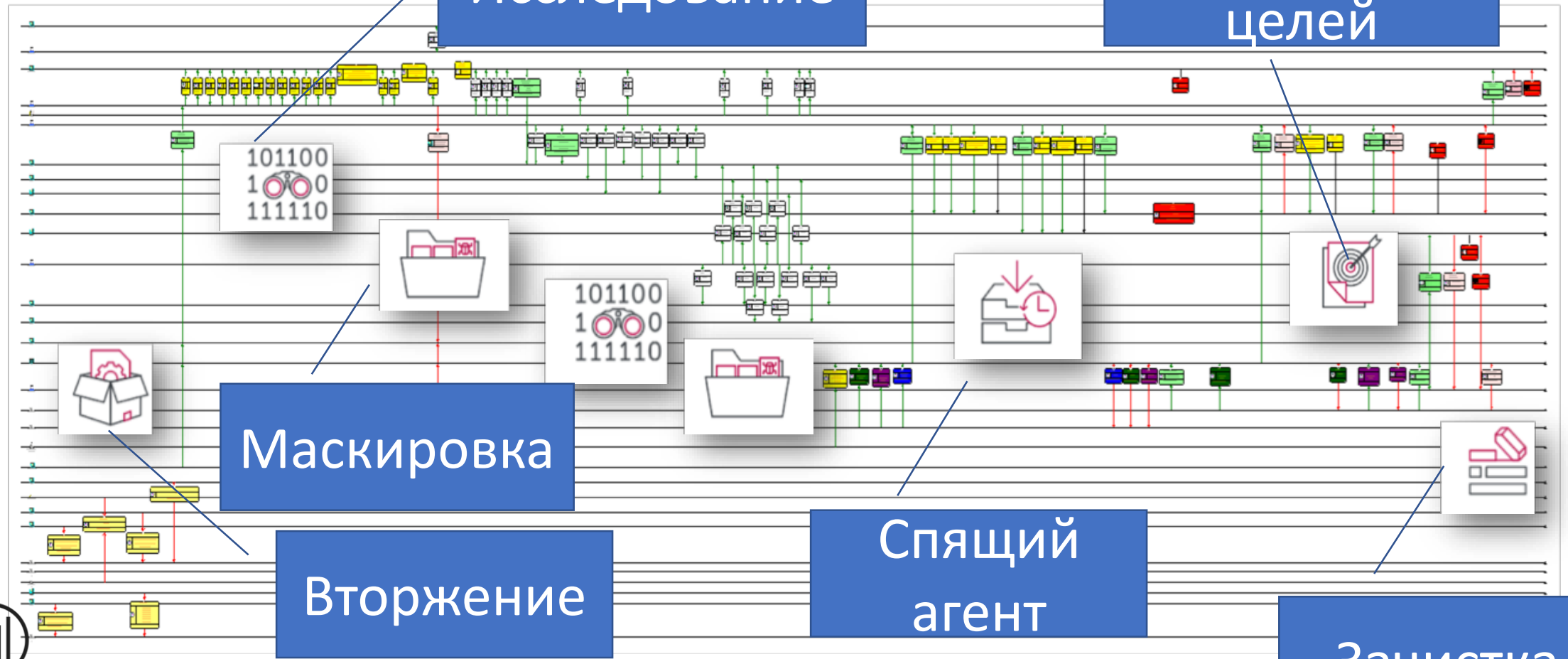




Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	98090	98304	7.15	2931e7424028d78effb101d98c680cee
.rsrc	102400	75372	75776	7.86	405f547c04e722b31ed7d770d752c6f8
.reloc	180224	1068	1536	4.32	5e004b89ac14a39595f48c00c2e3015e

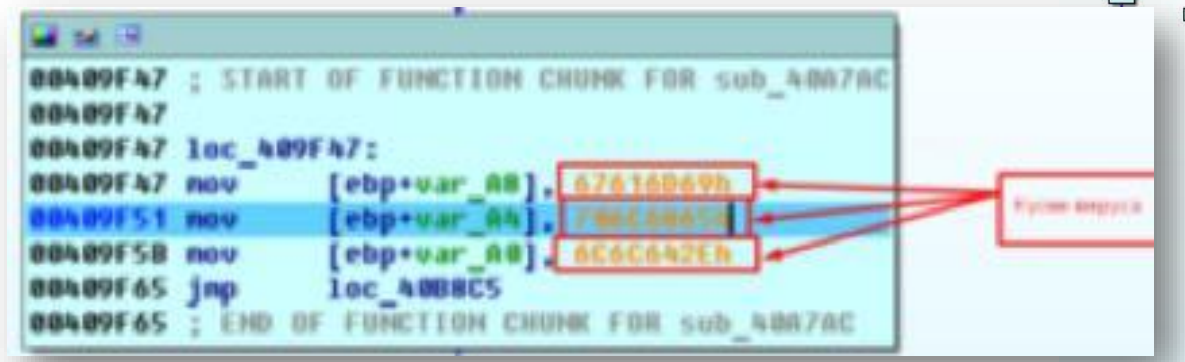
Advanced Technologies Solutions

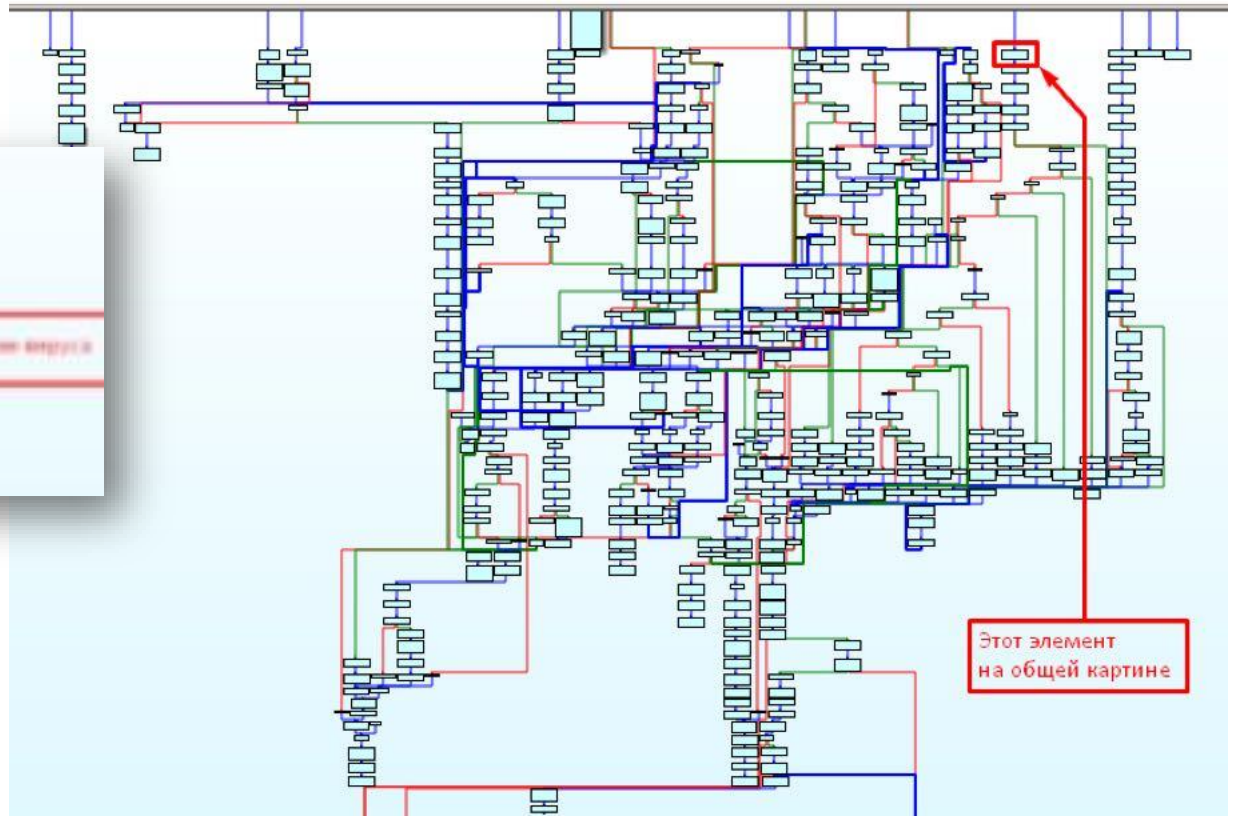
Пример отчета



Advanced Technologies Solutions

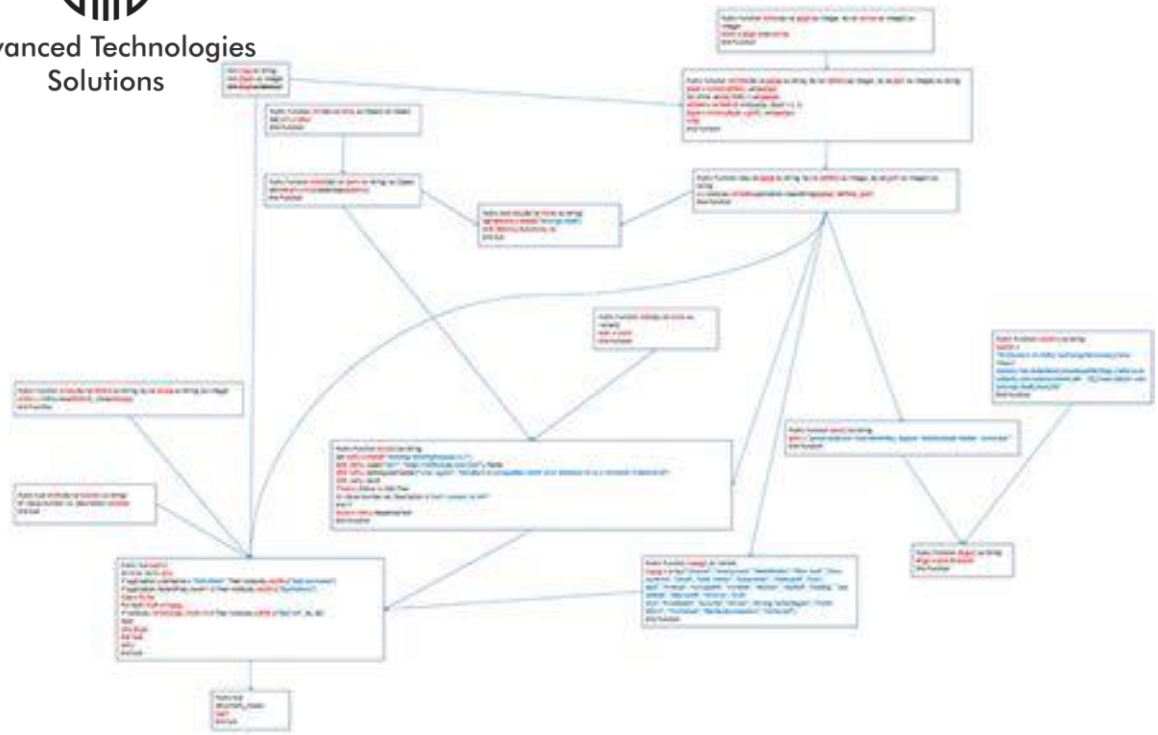
Advanced Technologies Solutions

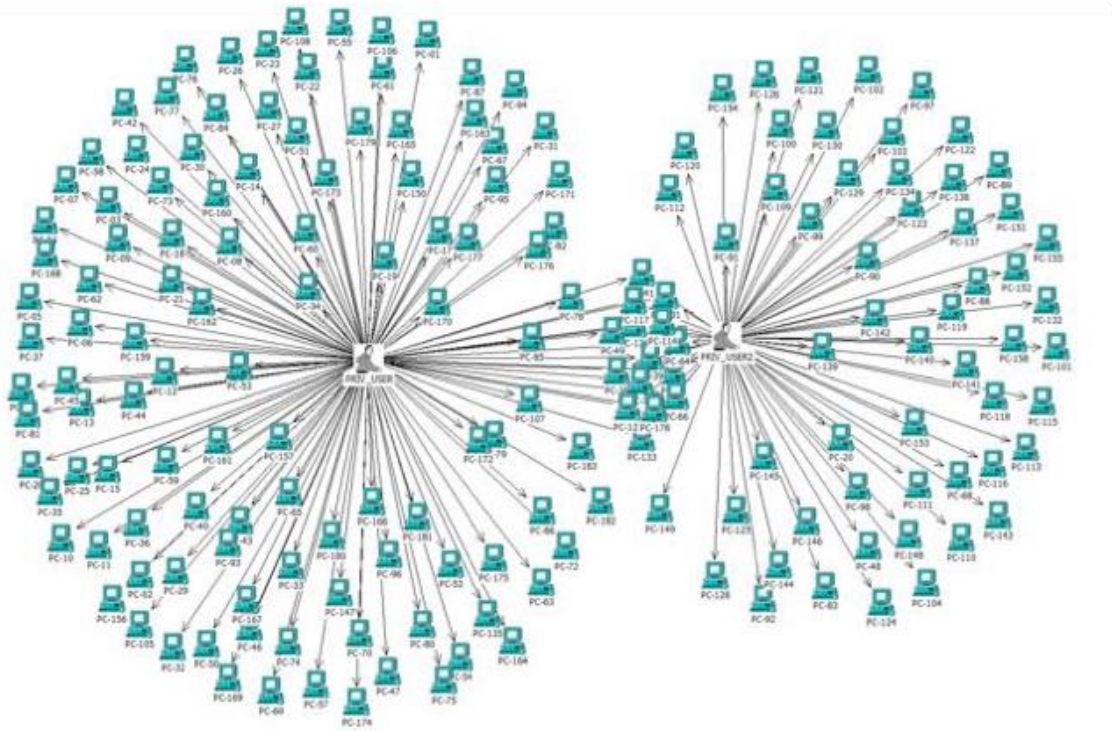




Пример отчета

Advanced Technologies Solutions





Визуализация деятельности

Aleksandr Tvaradze
at@atsol.az

Спасибо за внимание