T&T Security

DATA SHEET

tLab

Профессиональная защита от атак вредоносного ПО

Система tLab - передовой продукт по защите от киберугроз нового типа, против которых типичный антивирус малоэффективен: от атак нулевого дня, целевого вредоносного программного обеспечения (ВПО) и APT-атак.

Применимость

tLab – “Песочница” (sandbox), система глубокого анализа объектов обеспечивающая защиту Email и Web-трафика от вредоносных загрузок и вложений, опасных URL, скрытых и сложных атак ВПО (скрипты, приложения и

tLab в цифрах

- **Обнаруживает более 50 видов вредоносной активности**
- **Проверяет до 10000 файлов в день**
- **Вердикт на объект за 60 секунд**
- **На базе более 10 научных работ из США**

ИНТЕЛЛЕКТУАЛЬНОСТЬ

Глубокий анализ вредоносного поведения и эвристический анализ, которые обеспечивают распознавание сложных и скрытых атак ВПО

ПРОИЗВОДИТЕЛЬНОСТЬ

Быстрая оценка угрозы ВПО на основе комплексного, интерактивного отчета, позволяющего видеть угрозу изнутри

АВТОНОМНОСТЬ

Автоматизация защиты от ВПО путем интеграции с компонентами Mail/Web Gateway и сторонними решениями на основе REST API и стандартных протоколов

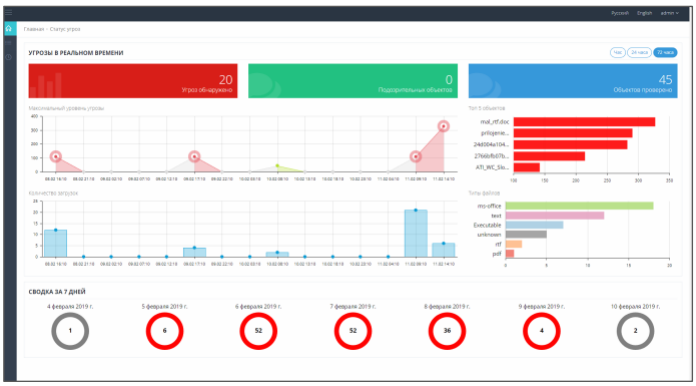
+7 (7172) 572190 Астана, Алпамыс 17 info@tntsecure.kz

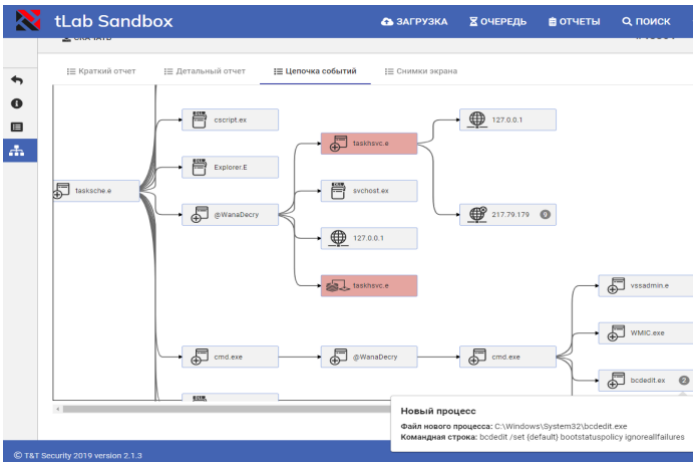
ПРЕИМУЩЕСТВА

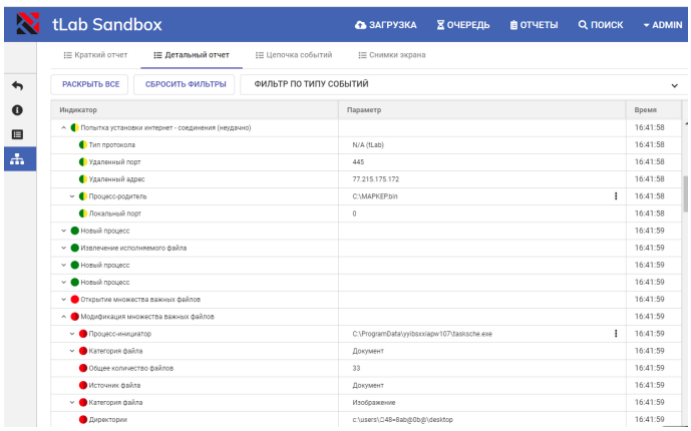
Передовое обнаружение атак

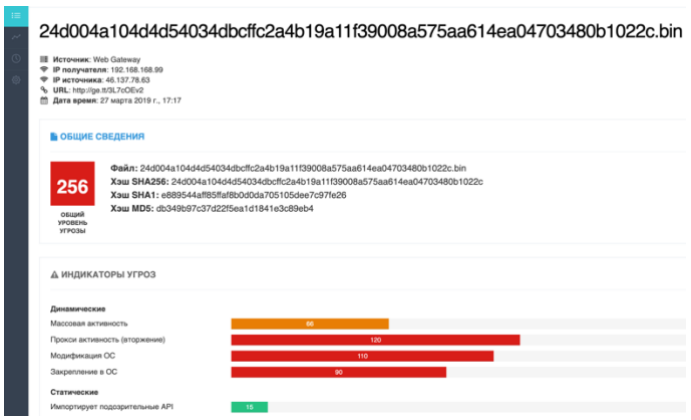
tLab идентифицирует ВПО путем глубокого анализа системного поведения программ в изолированной среде. Используется уникальная технология анализа поведения на уровне деревьев активности, которые описывают поток распространения вредоносной активности и взаимосвязи исполняемых объектов. Данная технология позволяет обнаружить скрытые и сложные вредоносные объекты, малозаметные для традиционных систем защиты.

tLab анализирует на вредоносность многие форматы файлов, включая, но не ограничиваясь: документы, скрипты, web-файлы, исполняемые, архивы и файлы клиентских приложений (eml).









Детальное исследование угроз

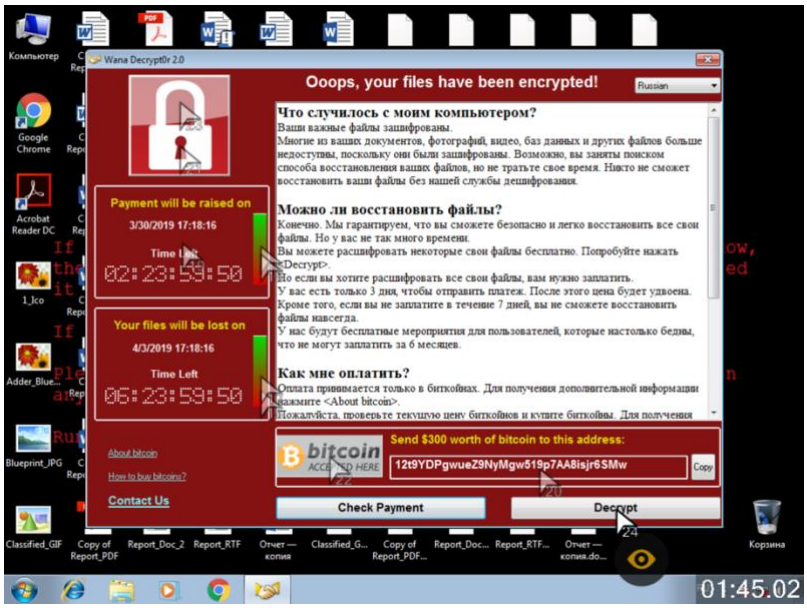
В отличие от классических песочниц, tLab не только обнаруживает и блокирует атаки в реальном времени, но и предоставляет мощный инструментарий для всестороннего исследования угрозы. tLab, идентифицирует уровень угрозы ВПО и предоставляет интерактивный отчет с визуализацией полной активности и указанием вредоносных функций.
Отчет содержит полную аналитику по ВПО различного уровня детализации включая статические характеристики, типы обнаруженных функциональностей, деревья активности (событий), контекста поведения объекта исследования, настройки среды исполнения и аспекты

ЗАЩИТА ОТ МАЛОЗАМЕТНЫХ АТАК

Продвинутая эмуляция активности пользователя (детонация ВПО)

Некоторые виды нежелательного и вредоносного ПО требуют взаимодействие с пользователем, соответственно такие образцы не будут активироваться (детонировать) пока пользователь не нажмет на соответствующие элементы графического интерфейса (кнопки, текстовые поля). К таким угрозам относиться троянские программы маскирующейся под легитимное ПО или нежелательное ПО, которое требует выполнения полного сценария инсталляции.
Также трояны-вымогатели могут требовать взаимодействия с пользователем для выполнения некоторых операций, например, обращение к серверу злоумышленника для загрузки информации по платежам-выкупа. Детонирование подобных объектов ВПО требует продвинутую и эффективную систему эмуляции пользователя как на уровне

Некоторые образцы ВПО, с целью обхода песочниц, демонстрируют пользователю статичное графическое изображение и не используют системные элементы управления, отслеживая нажатие пользователя на картинку кнопки. Песочницы не могут распознать элементы управления и соответственно не могут нажать и детонировать ВПО. tLab имеет в своем составе модуль распознавания образов для идентификации элементов



Режим анти-уклонения

tLab имеет возможность **противодействия** известным методам обнаружения и обхода песочниц, включая: обнаружение артефактов среды анализа, отложенное исполнение и продвинутый способ, использующий циклы микро-задержек. Данная технология противодействия обходу песочницы определяет эффективность при обнаружении скрытных целевых и нетипичных атак, которые, согласно мировой практики, составляют основу современной модели угроз ВПО.

ТЕХНИЧЕСКИЕ ВОЗМОЖНОСТИ

tLab обеспечивает загрузку объектов на анализ в следующих режимах:

- отправка файла в ручном режиме;
- загрузка с указанием командной строки запуска (входные аргументы);
- загрузка группы файлов с указанием запускаемого (для анализа файла с зависимостями);
- автоматическая отправка файлов через REST API (используется компонентами Web/Mail Gateway);
- загрузка и получение отчетов от продуктов TrendMicro (интеграция).

Симуляция (эмуляция) действий пользователей в среде исполнения tLab для активации ВПО:

- эмуляция пользователя по скриптам активности (выбор существующих или создание новых сценариев для контролируемой детонации (активации) объектов);
- эмуляция пользователя без скриптов (оптимальная активность);
- обнаружение скрытых угроз, использующих нетипичное диалоговое окно в виде статичной картинки.

tLab обеспечивает анти-уклонение - противодействие методам обнаружения и обхода песочниц:

- stealth-режим: скрытие артефактов файловой системы (файлы и процессы) для предотвращения обнаружения среды исполнения со стороны ВПО;
- камуфляж (динамическая подмена имени) артефактов реестра (ключи, значения и ветки) и устройств для предотвращения обнаружения среды исполнения со стороны ВПО;
- обнаружение объектов, использующих задержки исполнения (отложенный запуск), включая циклы микро-задержек. Данный функционал обеспечивает противодействия механизму обхода динамического анализа через отложенное исполненные путем сокращения времени ожидания.

Экспорт и отчетность в системе tLab:

- несколько уровней детализации поведенческого отчета (формирование интерактивных отчетов разного уровня детализации и информативности);
- интерактивная визуализация дерева событий - последовательность потенциально вредоносных действий с указанием их взаимосвязи (отслеживание источника и распространения вредоносной/подозрительной активности);
- обнаружение работы с важными файлами (открытие, модификация и удаление). отслеживается: тип источника, кол-во и категорию файлов (например, документ, аудио, бухгалтерия и т. д.);
- экспорт полного отчета в PDF документ на английском и русском языках;
- экспорт и импорт белого списка исключений (использование белых листов для идентификации некоторых легитимных файлов);
- доступ к идентифицированному вредоносному объекту (файлу) путем выгрузки с веб-интерфейса.

Проверка и анализ объектов в системе tLab:

- анализ файлов разных форматов – документы (rtf, pdf, xlsx, docx, pptx, xls, doc, ppt, xlsm, docm, pptm, pps, ppsx, ppsm, dot, dotm, odt, xps), веб-файлы (html, mht, mhtml), исполняемые файлы (exe, scr, dll, jar, msp, mst, msi, java, job, sct), скрипты (ps1, sh (linux batch script), js, vbs, bat, ws), архивы и файлы клиентских приложений (iso, bzip2, rar, zip, gzip, arj, 7z, cab, msg, eml);
- поведенческий анализ файлов проводится в операционных системах Windows включая: Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10;
- анализ по Yara-сигнатурам;
- глубокий анализ активности поведения исследуемых объектов (программ) с отслеживанием потока распространения вредоносной активности и поведенческой взаимосвязи исполняемых объектов;
- эвристический анализ скриптов - эмуляция хода исполнения и идентификация поведения скриптов (обнаружение супер-целевых угроз заточенных на наличие индикаторов конкретной группы машин, например, имя пользователей, путем эмуляции всех ветвлений кода);
- контекстный анализ документов для обнаружения вредоносного документа на уровне аномалии без сигнатур (позволяет обнаружить угрозу ВПО с эксплоитом нулевого дня);
- Статический и эвристический анализ документов различных типов (rtf, pdf, xlsx, docx, pptx, xls, doc, ppt, xlsm, docm, pptm).

ВНЕДРЕНИЕ И ИНТЕГРАЦИЯ

tLab обеспечивает **предотвращение атак ВПО**, распространяющихся по электронной почте и Веб путем интеграции с компонентами Mail и Web Gateway и сторонними решениями на основе REST API. Кроме того, система tLab поддерживает стандартные протоколы: ICAP для Web Gateway, SMTP в режиме BCC и IMAP с целью мониторинга угроз. В качестве Mail Gateway используется два решения на выбор: MTA-сервер либо плагин для почтового сервера MS Exchange.В качестве Web Gateway используется надежное open-source решение, включающее Next Generation Firewall (NGFW) и IPS с широким набором функционала.

Кроме того, имеется нативная интеграция с решениями Trend Micro для обеспечения безопасности во всех средах и сегментах инфраструктуры организации от сети до рабочих станций и серверов.

Данные решения проверяют каждый вложенный файл в песочнице и при выявлении угрозы вырезают опасные файлы из письма. Так же поддерживается возможность проверки группы файлов в одной среде, для обнаружения компонентных, распределённых атак. Система tLab имеет технологию контекстной анализа документов (Context Document Analysis), которая позволяет обнаружить вредоносные документы MS Office на основе валидации формата и идентификации аномалий. Это позволяет детально проверять документы с угрозами нулевого дня без использования сигнатур. Обновления tLab включают: семантические сигнатуры YARA (эксплоиты), сигнатуры сторонних/клиентских