

**KASPERSKY®**

**РУКОВОДСТВО  
ПО РЕАГИРОВАНИЮ  
НА ИНЦИДЕНТЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**

*Управление технологических решений*

*Версия 1.0 (07.02.2017)*

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО Kaspersky Lab (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

Дата редакции документа: 07.02.2017

© АО Kaspersky Lab, 2017.

<http://www.kaspersky.ru>

<https://help.kaspersky.com>

<http://support.kaspersky.ru>

# ОГЛАВЛЕНИЕ

Теоретическая часть .....	5
Определения .....	5
Введение .....	7
Цель и задачи данного документа .....	8
Жизненный цикл атаки (Kill Chain) .....	9
Разведка и сбор данных (Reconnaissance) .....	9
Выбор способа атаки (Weaponization) .....	10
Доставка (Delivery) .....	10
Эксплуатация (Exploitation) .....	10
Закрепление (Installation) .....	10
Исполнение команд (Command and Control) .....	10
Достижение цели (Actions on Objective) .....	10
Реагирование на инциденты ИБ .....	11
Цели процесса реагирования .....	11
Основные этапы процесса реагирования на инциденты ИБ .....	11
Инструкция по реагированию на инциденты .....	14
Подготовка .....	14
Обнаружение .....	15
События ИБ, свидетельствующие о возможном инциденте ИБ .....	15
Общие указания по приоритизации .....	15
Иные факторы, на которые следует обратить внимание при обнаружении угрозы .....	16
Алгоритм анализа событий в SIEM-системе .....	17
Сдерживание .....	19
Изоляция инфицированных машин .....	20
Снятие образов .....	20
Перевод системы в режим работы без изолированных машин .....	20
Удаление .....	20
Восстановление .....	21
Выводы .....	21
Рекомендуемые инструменты .....	22
Инструменты для первоначального реагирования .....	22
SysInternals .....	22
AVZ .....	23
Gmer .....	24
YARA .....	24
Инструменты для сбора данных .....	24

GRR Rapid Response .....	25
Forensic Toolkit .....	25
DD.....	25
Belkasoft RAM Capturer.....	26
Инструменты для анализа потенциальных угроз .....	26
Threat Lookup – Kaspersky Threat Intelligence Portal .....	26
Sandbox – Kaspersky Threat Intelligence Portal .....	27
Инструменты для анализа дампов памяти.....	27
Инструменты для анализа образов диска .....	29
Strings.....	30
Инструменты для удаления угроз .....	30
Kaspersky Virus Removal Tool .....	30
Kaspersky Rescue Disk.....	30
Специальные решения Лаборатории Касперского .....	31
Аналитические отчеты Лаборатории Касперского об угрозах класса APT .....	31
Пример реагирования на инцидент ИБ .....	32
Атака .....	32
Реагирование .....	34
Описание сетевой инфраструктуры.....	34
Обнаружение атаки .....	35
Реагирование на атаку .....	35
АО «Лаборатория Касперского» .....	40
Уведомление о товарных знаках .....	41

# ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## ОПРЕДЕЛЕНИЯ

ТЕРМИН	ОПРЕДЕЛЕНИЕ
<b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ)</b>	Сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под информационной безопасностью также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.
<b>СОБЫТИЕ ИБ</b>	Любое идентифицированное явление в системе или сети.
<b>ИНЦИДЕНТ ИБ</b>	Нарушение или угроза нарушения ИБ компании.
<b>УГРОЗА ИБ</b>	Потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента ИБ.
<b>УЯЗВИМОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ (ИС)</b>	Недостаток в ИС, используя который внешний злоумышленник может намеренно реализовать угрозу ИБ.
<b>ЭКСПЛОИТ (EXPLOIT)</b>	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на ИС.
<b>РЕАГИРОВАНИЕ НА ИНЦИДЕНТ ИБ</b>	Структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента ИБ.
<b>ЦЕЛЕВАЯ АТАКА</b>	Атака, нацеленная на одного человека, компанию или группу. В процессе атаки может использоваться различное вредоносное программное обеспечение и методы социальной инженерии.
<b>АРТ-АТАКА (ADVANCED PERSISTENT THREAT)</b>	Сложная, продолжительная, хорошо спланированная многоходовая атака, использующая сложное вредоносное ПО, методы социальной инженерии и данные об информационной инфраструктуре атакуемого.
<b>ЖИЗНЕННЫЙ ЦИКЛ АТАКИ (KILL CHAIN)</b>	Последовательность шагов осуществления атаки.

<b>SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)</b>	Система, которая обеспечивает анализ событий ИБ, исходящих от сетевых устройств и приложений, в реальном времени. Одной из возможностей SIEM-систем является сопоставление событий с потоками данных об угрозах.
<b>ИНДИКАТОРЫ КОМПРОМЕТАЦИИ (IOC)</b>	Наблюдаемая в компьютерной сети или на одном из компьютеров сущность, наличие которой может свидетельствовать о компрометации ИС. Обычно под такими индикаторами понимают IP-адреса, URL-адреса, хеши файлов.
<b>ПОТОКИ ДАННЫХ ОБ УГРОЗАХ (FEEDS)</b>	Информация, содержащая индикаторы компрометации и позволяющая выявлять факт компрометации, используя SIEM-системы и другие сетевые устройства и средства защиты информации.
<b>РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ (OSINT)</b>	Военный термин, применительно к ИБ означает поиск в открытых источниках необходимой информации, в том числе индикаторов компрометации, отчетов по конкретным угрозам и другой информации, которая может способствовать расследованию инцидента ИБ.
<b>АТАКА ТИПА WATERING HOLE</b>	Watering hole – одна из разновидностей многоуровневых целенаправленных кибератак. Атака заключается в том, что злоумышленники заражают вредоносным ПО веб-сайты, часто посещаемые их потенциальными жертвами. Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений.

## ВВЕДЕНИЕ

В последние годы число новых семейств и разновидностей вредоносного ПО стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Под угрозой находятся как домашние пользователи, так и крупные компании, банки, критическая инфраструктура, государственные организации, промышленные предприятия, использующие Автоматизированные системы управления технологическими процессами (АСУ ТП).

По данным исследовательского отчета<sup>1</sup> института Ponemon, средний ущерб от атак на ИС розничных магазинов за период только с 2013 по 2014 годы увеличился на 8 миллионов долларов и составил около 12 миллионов долларов на каждую крупную компанию. Среди финансовых организаций средний ущерб оценивался в 20,8 миллионов долларов, в технологическом секторе – 14,5 миллионов долларов в среднем на компанию.

Обнаруженный в 2010 году вирус Stuxnet стал первым вредоносным ПО, которое может быть использовано в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов. Уникальность программы заключалась в том, что впервые в истории вирус физически разрушал инфраструктуру и ставил под угрозу человеческие жизни. В результате действий Stuxnet 1368 из 5000 центрифуг по обогащению урана Натанзе были выведены из строя.

Чтобы защитить корпоративную сеть от различных угроз, многие организации применяют классические средства: антивирусные решения, сканеры безопасности, а также системы обнаружения и предотвращения вторжений. Однако указанные системы не всегда в состоянии обнаружить сложные целевые атаки или предоставить достаточное количество информации для приоритизации и расследования инцидентов ИБ, которые были обнаружены. Для этого сотрудники, отвечающие за информационную безопасность, должны использовать целый комплекс средств, чтобы обеспечить защиту ИС и ускорить расследование инцидентов ИБ, которые все же могут возникнуть. К таким средствам относятся:

- антивирусы на компьютерах и мобильных устройствах всех сотрудников;
- SIEM системы, в которые интегрированы потоки данных об угрозах;
- анти-APT-системы, обеспечивающие обнаружение сложных угроз и целевых атак;
- системы исследования образцов программного обеспечения и поиска подробной информации о характеристиках вредоносного программного обеспечения по индикаторам компрометации.

В момент возникновения инцидента от сотрудников, ответственных за ИБ, требуются быстрые и точные шаги, которые позволят минимизировать ущерб от инцидента и собрать доказательства для уголовного преследования злоумышленников. Для безошибочного совершения этих шагов необходимо наличие инструкции по реагированию на инциденты ИБ, созданной экспертами ИБ. Если сотрудники подразделений, ответственных за ИБ, не знают, как реагировать на возникший инцидент и как обеспечить оперативный сбор данных, необходимых для проведения расследования, атакованная организация понесёт значительные убытки. Ошибки в реагировании на инциденты ИБ приводят к достижению злоумышленником целей атаки и дают ему возможность для удаления следов своего присутствия в ИС.

---

<sup>1</sup> [https://ssl.www8.hp.com/us/en/ssl/leadgen/document\\_download.html?objid=4AA5-5208ENW](https://ssl.www8.hp.com/us/en/ssl/leadgen/document_download.html?objid=4AA5-5208ENW)

## ЦЕЛЬ И ЗАДАЧИ ДАННОГО ДОКУМЕНТА

Этот документ является кратким руководством по реагированию на инциденты ИБ.

**Документ предназначен для** руководителей и сотрудников подразделений, ответственных за ИТ и ИБ организаций.

**Задачами документа являются:**

- систематизация теоретической информации о жизненном цикле атаки и реагировании на инциденты ИБ;
- описание алгоритма реагирования на инциденты;
- описание инструментов, используемых на каждом этапе расследования инцидентов;
- знакомство читателя с практическими подходами к реагированию на инциденты.

Документ не является универсальной инструкцией по реагированию на всевозможные инциденты информационной безопасности, а представляет собой обзорное руководство по процессу реагирования на инциденты ИБ (Incident response).

**Для получения полной информации** по реагированию на инциденты сотрудникам и руководителям ИБ рекомендуется пройти обучение по направлениям:

- Реагирование на инциденты ИБ (Incident response).
- Цифровая криминалистика (Digital forensics).
- Анализ и обратная разработка вредоносного ПО (Advanced malware analysis & Reverse engineering).

«Лаборатория Касперского» предлагает тренинги любого уровня – от базового до экспертного – в области цифровой криминалистики и анализа вредоносного ПО. Курсы «Лаборатории Касперского» по кибербезопасности ориентированы на компании, которые стремятся защитить свою инфраструктуру и интеллектуальную собственность. Получить подробную информацию об обучении можно на сайте «Лаборатории Касперского»: <http://www.kaspersky.ru/enterprise-security/intelligence-services>.



## ЖИЗНЕННЫЙ ЦИКЛ АТАКИ (KILL CHAIN)

В процессе атаки злоумышленники осуществляют структурированную последовательность шагов, называемую kill chain. Первоначально kill chain использовался как военный термин для описания структуры военного вторжения. Зная последовательность действий противника, обороняющаяся сторона может выработать стратегию защиты и противостоять нападению. Впоследствии термин kill chain стал использоваться для описания компьютерных угроз. Аналогично, на основе информации об этапах компрометации ИС, сотрудники, ответственные за ИБ, могут выстраивать систему защиты ИС.



Рисунок 1: Жизненный цикл атаки (kill chain)

От того, на каком этапе kill chain была обнаружена угроза, зависит эффективность расследования и размер материального и репутационного ущерба, нанесённого атакуемой организации. Обнаружение на этапе достижения цели (позднее обнаружение) означает, что система ИБ ИС оказалась неспособна противостоять атаке и злоумышленник достиг поставленных целей. Наименьший ущерб будет нанесён в случае обнаружения на этапах Доставки или Закрепления (раннее обнаружение).

Далее приведено краткое описание каждого этапа стратегии угроз.

### РАЗВЕДКА И СБОР ДАННЫХ (RECONNAISSANCE)

На этом этапе происходит сбор информации об организации, которая будет атакована, а также о её информационных активах. В частности, злоумышленник пытается установить организационную структуру компании, стек технологий, используемый в атакуемой организации, средства обеспечения ИБ, возможности использования социальной инженерии по отношению к сотрудникам (например, выявить их аккаунты в социальных сетях).

Разведка может быть пассивной (Passive reconnaissance) и активной (Active reconnaissance). Пассивная разведка заключается в получении информации без непосредственного воздействия на атакуемую ИС (например, просмотр DNS и Whois информации, связанной с ИС организации). Активная разведка включает в себя взаимодействие с атакуемой ИС: сканирование портов, поиск уязвимостей ИС и другие действия.

Вся собранная злоумышленником информация служит источником знаний для следующего этапа.

## **ВЫБОР СПОСОБА АТАКИ (WEAPONIZATION)**

Используя информацию, полученную на этапе разведки и сбора данных, злоумышленник определяет способ атаки. При этом злоумышленник может создать новое вредоносное ПО, позволяющее эксплуатировать обнаруженные уязвимости.

Злоумышленник внедряет ПО, которое будет использоваться при атаке, в файлы MS Office (.docx, .xlsx), PDF-документы, электронные письма или на съёмные носители.

На этом же этапе происходит выбор способа доставки созданного вредоносного ПО в атакуемую организацию: с помощью заражения публичного ресурса компании, через одного из сотрудников или через компрометацию компаний-субподрядчиков, работающих с атакуемой организацией.

## **ДОСТАВКА (DELIVERY)**

Атакующий должен обеспечить попадание разработанного на прошлом шаге вредоносного ПО в ИС атакуемой организации. Обычно для этого используются вложения электронной почты, вредоносные и фишинговые ссылки, watering hole-атаки (заражения сайтов, которые посещают сотрудники атакуемой организации) или зараженные USB-устройства.

## **ЭКСПЛУАТАЦИЯ (EXPLOITATION)**

После попадания в ИС атакуемой организации вредоносное ПО, используя уязвимости ИБ, распространяется по сети и закрепляется на зараженных машинах в ожидании команд, поступающих от злоумышленника.

Команды от злоумышленника могут поступать как через интернет (от командных центров C&C), так и с помощью доставки другого вредоносного ПО (например, если на машине отсутствует прямое подключение к интернету).

## **ЗАКРЕПЛЕНИЕ (INSTALLATION)**

Вредоносное ПО осуществляет заражение компьютера для того, чтобы не быть обнаруженным или удаленным после перезагрузки или установки обновления, блокирующего возможность использовать одну из уязвимостей ИС. Обычно для заражения используются утилиты несанкционированного управления (backdoor).

## **ИСПОЛНЕНИЕ КОМАНД (COMMAND AND CONTROL)**

С помощью соединения, устанавливаемого изнутри ИС атакованной организации, вредоносное ПО реализует взаимодействие с сервером управления, подконтрольным злоумышленнику (C&C Server). Таким образом, атакующий получает управление компьютером внутри ИС атакуемой организации.

## **ДОСТИЖЕНИЕ ЦЕЛИ (ACTIONS ON OBJECTIVE)**

Получив управление, злоумышленник может работать с данными на скомпрометированном компьютере, не только осуществляя несанкционированный доступ, но и изменяя или удаляя их. Кроме того, атакующий может попытаться заразить другие машины в ИС, для того чтобы увеличить объем доступной информации.

## РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ

В этом разделе описаны общие шаги, необходимые при реагировании на инциденты ИБ.

### ЦЕЛИ ПРОЦЕССА РЕАГИРОВАНИЯ

Основными целями реагирования на инциденты ИБ являются минимизация ущерба, скорейшее восстановление исходного состояния ИС и разработка плана по недопущению подобных инцидентов в будущем. Эти цели достигаются на двух основных этапах: расследование инцидента и восстановление системы.

При расследовании требуется определить:

- начальный вектор атаки;
- вредоносные программы и инструменты, которые были использованы в процессе атаки;
- какие системы были затронуты в ходе атаки;
- размер ущерба, нанесенного атакой;
- завершена атака или нет, то есть достиг ли атакующий своей цели;
- временные рамки атаки.

После завершения расследования необходимо разработать и внедрить план восстановления системы, используя информацию, полученную при расследовании.

### ОСНОВНЫЕ ЭТАПЫ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

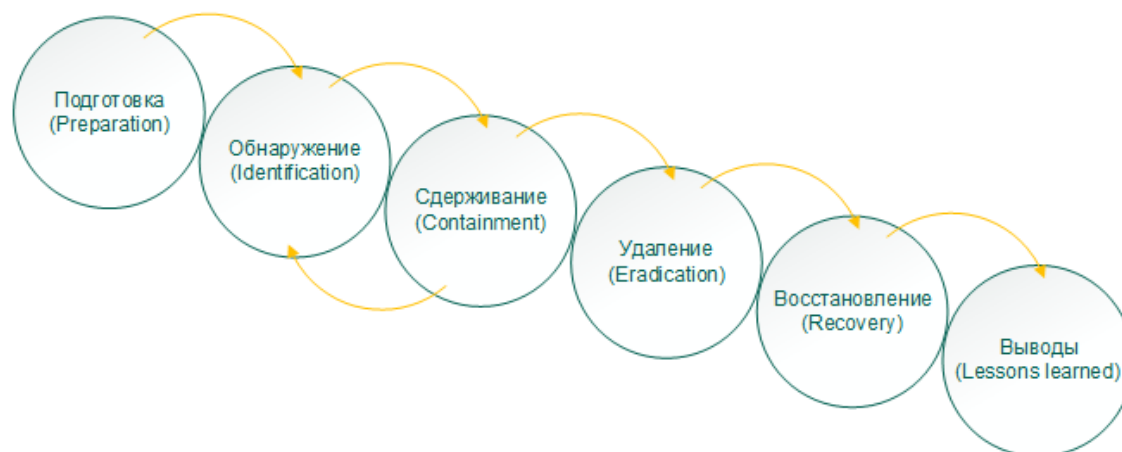


Рисунок 2: Процесс реагирования на инциденты ИБ

На основе информации о жизненном цикле атаки (kill chain), возможно формирование системы защиты. Исходя из анализа стратегии, используемой при атаке на ИС, специалистами ИБ выработана стратегия реагирования на инциденты, которая будет описана ниже.

#### Подготовка (Preparation)

В момент, когда происходит инцидент ИБ, от сотрудников, ответственных за ИБ, требуются моментальные и точные действия. Поэтому для эффективного реагирования необходима предварительная подготовка. Сотрудники, ответственные за ИБ, должны обеспечить защиту ИС и проинформировать пользователей, а также ИТ-персонал, о важности мер по обеспечению ИБ. Сотрудники, занимающиеся реагированием на инциденты ИБ, должны пройти соответствующее обучение и регулярно посещать тренинги по ИБ, для того чтобы оперативно и эффективно реагировать на инциденты ИБ.

## Обнаружение (Identification)

Сотрудники, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения ИБ событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов ПО и другие источники информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы (IOC).



Рисунок 3: Цикл обнаружения индикаторов компрометации

Сбор индикаторов компрометации является итерационным процессом. На основе первоначальной информации, полученной от SIEM-системы, происходит формирование сценариев обнаружения, применение которых, как правило, приводит к выявлению новых индикаторов компрометации. Полученные таким образом индикаторы помогают уточнить границы атаки и служат отправной точкой для нового цикла обнаружения.

Дальнейшие шаги предпринимаются только если событие решено считать инцидентом ИБ.

## Сдерживание (Containment)

Сотрудники, ответственные за ИБ, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИС компании могла продолжать работать без зараженных машин.

## Удаление (Eradication)

Цель этого этапа – привести скомпрометированную ИС в состояние, в котором она была до заражения. Сотрудники, ответственные за ИБ, удаляют вредоносное ПО, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИС.

## Восстановление (Recovery)

Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом сотрудники, ответственные за ИБ, некоторое время продолжают наблюдать за состоянием этих машин и ИС в целом, чтобы убедиться в полном устранении угрозы.

## Выводы (Lessons learned)

Сотрудники, ответственные за ИБ, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию ПО и оборудования, обеспечивающего ИБ, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

# ИНСТРУКЦИЯ ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

В этом разделе приведено описание рекомендаций и инструментов, которые позволят повысить эффективность реагирования на инциденты ИБ.

## ПОДГОТОВКА

Для того чтобы эффективно противостоять угрозам ИБ, рекомендуется обеспечить защиту ИС на всех уровнях. На рабочих станциях рекомендуется установить Endpoint-антивирусы. В сети ИС должны присутствовать IPS, FireWall, Proxy с авторизацией, анти-APT-решения, SIEM с интегрированными потоками данных об угрозах, системы сетевых ловушек и другие системы ИБ.

Специалисты «Лаборатории Касперского» непрерывно разрабатывают различные средства обеспечения ИБ, в том числе антивирус для рабочих станций [Kaspersky Endpoint Security](#), который обеспечивает комплексную защиту компьютера от различных видов угроз, сетевых и мошеннических атак. Для противодействия целенаправленным атакам и передовым угрозам информационной безопасности эксперты «Лаборатории Касперского» создали продукт [Kaspersky Anti Targeted Attack Platform](#) (КАТА), который позволяет обнаружить комплексные целевые атаки. С информацией о решениях «Лаборатории Касперского» для крупного бизнеса можно ознакомиться на сайте <http://www.kaspersky.ru/enterprise-security>.

Повышению безопасности ИС также способствует проведение тестов на проникновение в ИС данной компании (penetration testing) и ознакомление специалистов, обеспечивающих ИБ, с отчетами по тестированию на проникновение. Тестирование может быть проведено сторонними организациями, а информация из отчетов поможет выявить и устранить уязвимости в ИС организации.

Специалисты, отвечающие за ИБ, должны регулярно повышать свою квалификацию на различных тренингах и семинарах, следить за последними тенденциями ИБ и быть в курсе новейших программных и аппаратных решений в области ИБ, а также отслеживать появляющиеся новые типы угроз и сценарии атак. Например, Global Research and Analysis Team (GReAT) «Лаборатории Касперского» регулярно публикует [отчёты](#) на портале APT Intelligence.

Для отслеживания и ведения статистики инцидентов ИБ необходимо выработать процедуру реагирования на инциденты ИБ, а также выбрать средство накопления и хранения экспертной информации и отчетов о произошедших ранее инцидентах ИБ. Такая информация позволит ускорить расследования инцидентов ИБ в будущем.

## ОБНАРУЖЕНИЕ

### СОБЫТИЯ ИБ, СВИДЕТЕЛЬСТВУЮЩИЕ О ВОЗМОЖНОМ ИНЦИДЕНТЕ ИБ

К источникам событий ИБ относятся Anti-APT-системы, сетевые ловушки (honeypot), системы обнаружения вторжений и многие другие решения для обеспечения ИБ (security controls). В рамках этого руководства область источников событий сужена до SIEM-систем (SIEM поддерживают интеграцию с различными программными и аппаратными решениями обеспечения ИБ, в том числе прокси-серверами, брандмауэрами и другими) и систем централизованного управления корпоративными Endpoint-антивирусами.

Соответственно триггерами для начала реагирования на инцидент будут следующие события:

- Событие в SIEM, возникающее в результате сопоставления событий от устройств обеспечения ИБ с потоками данных об угрозах. Такое событие свидетельствует о наличии в исходном событии от устройства обеспечения ИБ (например, прокси-сервера) одного из индикаторов, содержащихся в потоках данных об угрозах «Лаборатории Касперского».
- Некоторые срабатывания антивируса на Endpoint-компьютере (информация о срабатывании отображается в центре управления антивирусами). Реагировать на это событие нужно точно таким же образом, как при получении события в SIEM, содержащего хеш<sup>2</sup> вредоносного объекта.  
Не всякое срабатывание антивируса должно инициировать процесс реагирования на инциденты. Требуемыми расследования можно считать следующие срабатывания:
  - обнаружение взаимодействия с сервером управления C&C;
  - безуспешное лечение зараженных объектов;
  - неоднократное заражение одного и того же компьютера;
  - ошибки в работе антивируса, которые приводят к снижению уровня защищённости.

Эти триггеры почти всегда свидетельствуют о наличии инцидента ИБ. Однако не следует опираться только на них.

О наличии инцидента могут свидетельствовать и иные события, наличие которых должно заставить сотрудника, ответственного за ИБ, более внимательно отнестись к исследованию данного события ИБ, например:

- наличие неизвестного ПО в списках автозагрузки;
- появление неизвестных сервисов в списке сервисов ОС;
- запуск исполняемых файлов из папок, в которых ПО обычно не располагается (например, временные папки системы, системный кеш и другие);
- загрузка динамических библиотек из папок, в которых обычно данные библиотеки не располагаются (например, загрузка системных библиотек из папки, в которой располагается загружающий их исполняемый файл);
- непредвиденная или необычная сетевая активность;
- непредвиденное повышение привилегий пользователя.

### ОБЩИЕ УКАЗАНИЯ ПО ПРИОРИТИЗАЦИИ

Время является одним из самых дефицитных ресурсов при реагировании на инциденты; от скорости реакции сотрудников ИБ зависит то, успеет атака достичь целей или нет. Однако в случае большого числа инцидентов реагировать на все инциденты сразу невозможно. В такой ситуации необходимо приоритезировать инциденты.

Приоритет инцидента выставляется в зависимости от сегмента сети (определяется не только физическим положением компьютера в сети, но и ценностью данных, которые размещены на потенциально скомпрометированной машине), в котором произошел инцидент, типа и количества

---

<sup>2</sup> Для получения хеша можно использовать утилиты Certutil [Win], md5sum [\*nix].

инцидентов, а также от показателя достоверности индикатора, по которому был выявлен инцидент.

Определять, какие инциденты следует расследовать в первую очередь, следует исходя из специфики конкретной организации. В некоторых случаях наибольшую опасность могут представлять инциденты, в которых были обнаружены вирусы-шифровальщики (Ransomware), в других – инциденты с ПО, относящимся к категории условно опасных программ.

В качестве примера приоритизации можно привести подход, при котором в первую очередь должны быть расследованы инциденты, в которых есть подозрения на АРТ-угрозы (способы определения АРТ-угроз перечислены ниже), затем следует переключиться на инциденты, связанные с вредоносными ПО. Последними расследуются инциденты, связанные с ПО, относящимся к категориям условно опасных угроз (Adware, Pornware и подобных).

## Способы определения АРТ-угроз

Для того чтобы определить, является ли АРТ-угрозой обнаруженная в рамках инцидента ИБ угроза, рекомендуется воспользоваться следующими критериями:

1. Наличие индикаторов компрометации, соответствующих обнаруженному образцу в аналитических отчётах «Лаборатории Касперского» об АРТ-угрозах (см. [Аналитические отчеты Лаборатории Касперского об угрозах класса АРТ](#)). Подробнее о том, как осуществить сбор индикаторов, см. раздел [Инструменты для первоначального реагирования](#).
2. Взаимодействие угрозы с серверами управления (C&C Servers), которые ранее использовались АРТ-угрозами, выявляемое с использованием статического или динамического анализа угрозы. Для того чтобы определить поведение угрозы и список url-адресов, с которыми она взаимодействует, рекомендуется воспользоваться инструментами, описанными в разделе [Инструменты для анализа потенциальных угроз](#).

Угрозы, индикаторы компрометации которых имеют значение популярности 2 и более в потоках данных об угрозах «Лаборатории Касперского», относятся к массовому вредоносному ПО. Такие угрозы не могут считаться АРТ, и на них необходимо реагировать как на массовое вредоносное ПО. Также для оценки популярности угрозы рекомендуется воспользоваться решением [Threat Lookup – Kaspersky Threat Intelligence Portal](#). Если популярность индикатора компрометации (хеш-сумма, URL-адрес) низкая, возможно, индикатор относится к АРТ-угрозе.

## ИНЫЕ ФАКТОРЫ, НА КОТОРЫЕ СЛЕДУЕТ ОБРАТИТЬ ВНИМАНИЕ ПРИ ОБНАРУЖЕНИИ УГРОЗЫ

Ниже приведены примеры поведения ПО, которое может свидетельствовать о наличии инцидента ИБ. **Данный список не является полным перечнем подозрительного поведения.**

1. Взаимодействие потенциальной угрозы с доменами, которые часто меняют IP-адрес. Данный факт может свидетельствовать об использовании злоумышленником Fast flux DNS с целью сокрытия реального положения сервера управления.
2. Обращения к URL-адресам, которые категорированы в потоках данных об угрозах «Лаборатории Касперского». Например, Malware source, Exploit pack landing page и другие.
3. Обращения к IP-адресам, которые категорированы в потоках данных об угрозах «Лаборатории Касперского». Например, NetScanner (IP, с которых производится сканирование сети), DDoS amplifier (IP, с которого производилась DDoS-атака) и другие.
4. Дата регистрации, контактное лицо и контактные данные, которые указаны в Whois-информации о домене, с которым взаимодействует потенциальная угроза.
5. Записи о непредвиденных повышениях привилегий пользователей ИС.
6. Увеличение объема трафика по протоколам DNS или/и ICMP.
7. Детектирование образцов подобных mimikatz, Windows® Credentials Editor (WCE) и инструментов удаленного администрирования.



## АЛГОРИТМ АНАЛИЗА СОБЫТИЙ В SIEM-СИСТЕМЕ

Сотруднику ИБ при получении сообщения о детектировании угрозы в SIEM-системе рекомендуется выполнить следующую последовательность действий:

1. Попытаться определить источник исходного события, которое было сопоставлено с потоками данных об угрозах, то есть установить событие, содержащее обнаруженный индикатор компрометации:
  - 1.1. Если доставка угрозы произошла через рассылку электронных писем с опасными вложениями, то это можно будет обнаружить по журналам корпоративной почтовой системы.
  - 1.2. В случае заражения в процессе серфинга сети Интернет – индикаторы компрометации обнаруживаются в журналах прокси-сервера (файрволла, шлюза безопасности UTM или других устройств).
2. Определить, на каком этапе жизненного цикла находится обнаруженная атака. Это зависит от типов обнаруженных индикаторов, например, если было обнаружено взаимодействие с C&C-серверами, то атака находится на этапе исполнения команд и требует незамедлительных шагов для минимизации ущерба.
3. Оценить важность информации на потенциально скомпрометированной машине и показатель достоверности индикатора, по которому был выявлен инцидент, скорректировать приоритет данного инцидента в зависимости от ценности затронутых информационных активов и информации об индикаторе.

Дальнейшие шаги зависят от типа угрозы, которая была обнаружена в потоках данных об угрозах.

Для тех угроз, которые могли быть заблокированы Endpoint-антивирусом (например, Phishing-страница или Malicious-файл), следует проводить расследование в том случае, если:

- угроза не была заблокирована антивирусом (то есть пользователь открыл веб-страницу или загрузил файл);
- угроза была заблокирована, но подобное событие уже возникало раньше (например, на одном и том же компьютере постоянно блокируется скачивание Malicious-файла).

### Обнаружен URL-адрес угрозы

Ниже рассмотрены категории опасных URL, которые могут быть обнаружены при сопоставлении событий в SIEM с потоками данных об угрозах «Лаборатории Касперского».

КАТЕГОРИЯ УГРОЗЫ	НЕОБХОДИМЫЕ ШАГИ
<b>PHISHING</b>	<ol style="list-style-type: none"> <li>1. Исследовать исходный код web-страницы, на которую ведет опасный URL. Определить, какие данные пользователь мог передать злоумышленникам.</li> <li>2. В SIEM проанализировать события, связанные с пользователем, инициировавшим обращение на Phishing URL, в десятиминутном интервале. <ol style="list-style-type: none"> <li>2.1. Если были загружены или отправлены какие-либо файлы, повторить этап обнаружения для их индикаторов.</li> <li>2.2. В противном случае довести до сведения пользователя, инициировавшего активность, информацию об инциденте.</li> </ol> </li> <li>3. Если есть угроза компрометации, следует сменить пароли данного пользователя в ИС.</li> </ol>
<b>MALICIOUS</b>	<ol style="list-style-type: none"> <li>1. По событиям Proxy-сервера проверить, было ли получено вредоносное ПО. Если вредоносное ПО не было получено, значит заражения не произошло. Такое событие не является инцидентом, и дальнейшее расследование не проводится. URL при этом нужно занести в черный список.</li> <li>2. Убедиться, что вредоносное ПО не было заблокировано какими-либо средствами обеспечения ИБ (Proxy, Endpoint-антивирус). Если угроза была заблокирована, значит заражения не было и дальнейшее расследование не проводится. Исключением являются случаи повторного заражения – их следует расследовать в любом случае.</li> <li>3. Получить образцы вредоносного ПО по ссылке.</li> <li>4. Исследовать исходный код web-страницы по ссылке.</li> <li>5. Исследовать образец вредоносного ПО (см. <a href="#">Инструменты для анализа потенциальных угроз</a>).</li> <li>6. Проверить, был ли запущен скачанный образец (если возможно).</li> <li>7. Просканировать на наличие обнаруженных индикаторов диск компьютера, на котором была обнаружена угроза (см. <a href="#">Инструменты для анализа образов диска</a>) и машины в сегменте сети.</li> </ol> <p>Затем перейти к этапу <a href="#">Сдерживание</a>.</p>
<b>BOTNET C&amp;C</b>	<p><b>Обратите внимание.</b> Обращения к C&amp;C-адресам свидетельствует о наличии активного заражения.</p> <ol style="list-style-type: none"> <li>1. Выявить ПО, инициировавшее запросы к C&amp;C и исследовать его (см. <a href="#">Инструменты для анализа потенциальных угроз</a>).</li> <li>2. Просканировать инициировавший активность компьютер на наличие вредоносного ПО, которое могло быть загружено по командам от сервера управления.</li> <li>3. Исследовать URL (см. <a href="#">Инструменты для анализа потенциальных угроз</a>).</li> <li>4. Просканировать на наличие обнаруженных индикаторов диск (см. <a href="#">Инструменты для анализа образов диска</a>) и машины в сегменте сети.</li> </ol> <p>Затем перейти к этапу <a href="#">Сдерживание</a>.</p>
<b>MOBILE BOTNET C&amp;C</b>	<ol style="list-style-type: none"> <li>1. Просканировать телефон, который инициировал соединение с C&amp;C адресом, мобильным антивирусом.</li> </ol> <p>Затем перейти к этапу <a href="#">Сдерживание</a>.</p>

## Обнаружен хеш вредоносного объекта

Ниже рассмотрены категории опасных хеш-сумм, которые могут быть обнаружены при сопоставлении событий в SIEM с потоками данных об угрозах «Лаборатории Касперского».

КАТЕГОРИЯ УГРОЗЫ	НЕОБХОДИМЫЕ ШАГИ
<b>MALICIOUS, BOT</b>	<ol style="list-style-type: none"><li>1. Исследовать образец (см. <a href="#">Инструменты для анализа потенциальных угроз</a>).</li><li>2. Просканировать на наличие обнаруженных индикаторов диск (см. <a href="#">Инструменты для анализа образов диска</a>) и машины в сегменте сети.</li></ol> <p>Затем перейти к этапу <a href="#">Сдерживание</a>.</p>
<b>MOBILE MALICIOUS, BOT, TROJAN</b>	<ol style="list-style-type: none"><li>1. Просканировать телефон, на котором был обнаружен хеш вредоносного объекта, мобильным антивирусом.</li></ol> <p>Затем перейти к этапу <a href="#">Сдерживание</a>.</p>

## Обнаружен IP-адрес вредоносного объекта

Ниже рассмотрены категории зловредных IP, которые могут быть обнаружены при сопоставлении событий в SIEM с потоками данных об угрозах «Лаборатории Касперского».

КАТЕГОРИЯ УГРОЗЫ	НЕОБХОДИМЫЕ ШАГИ
<b>TOR EXIT NODE</b>	<ol style="list-style-type: none"><li>1. Запросить от пользователя подтверждение использования сети Tor®<ol style="list-style-type: none"><li>1.1. В случае, если пользователь подтверждает, что использует Тор, дальнейшее расследование не проводится, инцидент считается закрытым.</li><li>1.2. В противном случае просканировать машину пользователя (см. <a href="#">Инструменты для первоначального реагирования</a>) и машины в сегменте сети, а затем повторить этап обнаружения для детектированных файлов.</li></ol></li></ol>
<b>SPAM</b>	Перейти к этапу « <a href="#">Выводы</a> ».
<b>MALWARE</b>	<ol style="list-style-type: none"><li>1. Выявить ПО, инициировавшее запросы к детектированному IP-адресу, исследовать его (см. <a href="#">Инструменты для анализа потенциальных угроз</a>).</li></ol> <p>Дальнейшие шаги аналогичны обнаружению Malicious URL-адреса.</p>

## СДЕРЖИВАНИЕ

Цель этого этапа заключается не только в том, чтобы изолировать скомпрометированные компьютеры, но и в том, чтобы не допустить уничтожения индикаторов компрометации, которые

могут помочь в расследовании инцидента. Некоторые угрозы не создают файлов на диске, а полностью размещают себя в оперативной памяти, так как там их сложнее обнаружить. Поэтому недопустимо отключать питание компьютера, так как при этом будет утрачена вся информация, содержащаяся в оперативной памяти.

## **ИЗОЛЯЦИЯ ИНФИЦИРОВАННЫХ МАШИН**

Рекомендуется вывести инфицированные компьютеры в отдельную сеть. В случае, если есть подозрение на APT-атаку, не следует физически отключать компьютер от локальной сети (извлечением провода). Некоторые виды угроз отслеживают наличие сетевого соединения и могут начать уничтожение следов в случае, если сеть была отключена на длительное время. Вместо этого следует перенастроить правила маршрутизации таким образом, чтобы инфицированные машины не смогли коммуницировать с другими компьютерами организации.

## **СНЯТИЕ ОБРАЗОВ**

Для дальнейшего расследования необходимо получить дампы оперативной памяти и диска скомпрометированного компьютера. Снятие образов позволяет получить все компоненты вредоносного ПО. По результатам исследования этих компонентов можно определить, как следует бороться с заражением. Также анализ образов позволит определить вектор распространения угрозы, чтобы не допустить повторного заражения по аналогичному сценарию.

В случае, если передача данных затруднена (например, организация имеет несколько географически распределенных офисов и сотрудники, ответственные за реагирование на инциденты, есть только в некоторых из них), необходимо в первую очередь передать для исследования дампы оперативной памяти и лишь затем принять решение о необходимости снятия полного образа диска. При снятии образа диска записывается полный образ диска (в том числе с неиспользуемых секторов), а не только видимая пользователю часть, поэтому необходим носитель информации, превышающий общую емкость жесткого диска.

Для снятия образа рекомендуется использовать средства, описанные в разделе [Инструменты для сбора данных](#).

## **ПЕРЕВОД СИСТЕМЫ В РЕЖИМ РАБОТЫ БЕЗ ИЗОЛИРОВАННЫХ МАШИН**

Проведение этапа восстановления займет некоторое время. На это время ИС должна быть сконфигурирована так, чтобы отсутствие пораженных машин минимально влияло на функционирование ИС.

## **УДАЛЕНИЕ**

Существуют две стратегии проведения данного этапа – полное восстановление из образа рабочей станции или обнаружение и удаление угрозы и всех её артефактов (набор артефактов определяется по результатам анализа с помощью средств из раздела [Инструменты для анализа потенциальных угроз](#)).

Для удаления угрозы с компьютера рекомендуется использовать утилиты, описанные в разделе [Инструменты для удаления угроз](#) (например, Endpoint-антивирус).

В корпоративных сетях, где рабочее место пользователя стандартизовано, может оказаться, что эффективнее вместо этапов сдерживания, удаления и восстановления полностью переустановить операционную систему и ПО на скомпрометированных пользовательских рабочих станциях (образцы вредоносного ПО при этом необходимо сохранить для расследования). В случае заражения мобильного устройства эффективнее может быть проведение процедуры аппаратного сброса.

## ВОССТАНОВЛЕНИЕ

После успешного проведения этапа удаления необходимо ввести машины обратно в сеть. При этом сотрудники, ответственные за ИБ, должны некоторое время внимательно наблюдать за состоянием сети и восстановленных машин, чтобы убедиться в том, что угроза была полностью устранена.

## ВЫВОДЫ

По результатам расследования инцидента сотрудники, ответственные за ИБ, готовят отчет. Содержание отчета должно отвечать на вопросы:

- Когда, кем, и с помощью каких инструментов был впервые обнаружен инцидент?
- Что включал в себя инцидент?
- Как проводилось сдерживание, удаление и восстановление?
- На каких этапах реагирования сотрудники, ответственные за ИБ, были наиболее эффективны?
- Что необходимо улучшить в работе сотрудников, ответственных за ИБ?

Также на этом этапе необходимо подготовить рекомендации по повышению ИБ ИС. Рекомендации основываются на информации о способах доставки и закрепления угрозы, полученной в ходе расследования. Такие рекомендации позволяют дополнить правила устройств, обеспечивающих ИБ, новыми правилами и индикаторами угроз, в том числе расширить черные списки полученными индикаторами, например, URL- и IP-адресами, хеш-суммами угроз.

Выводы также могут повлечь обновление регламентов и правил пользования ИС организации. В таком случае новые правила должны быть доведены до сведения всех сотрудников компании и отражены в бизнес-логике ИС.

# РЕКОМЕНДУЕМЫЕ ИНСТРУМЕНТЫ

В этом разделе приведены описания инструментов, упомянутых в главе «[Инструкция по реагированию на инциденты](#)». Утилиты, представленные в этом разделе, являются примерами инструментов, которые используются при реагировании на инциденты.

Некоторые описанные ниже утилиты разработаны сторонними компаниями. Лаборатория Касперского не несёт ответственность за работоспособность и качество работы стороннего ПО. Полное описание утилит доступно на сайтах компаний-разработчиков.

Для получения дополнительной информации о продуктах и решениях «Лаборатории Касперского», описанных в этом разделе вы можете связаться с [intelligence@kaspersky.com](mailto:intelligence@kaspersky.com) или посетить сайт <http://www.kaspersky.ru/enterprise-security/intelligence-services>.

## ИНСТРУМЕНТЫ ДЛЯ ПЕРВОНАЧАЛЬНОГО РЕАГИРОВАНИЯ

Большинство атак проходит через этапы kill chain, перечисленные [выше](#). При этом на каждом этапе вредоносное ПО оставляет на скомпрометированной машине следы, называемые индикаторами компрометации (IOCs). При расследовании инцидентов необходимо обнаружить такие индикаторы, определить этап атаки, которому они соответствуют, выявить уязвимости, использованные вредоносным ПО и предотвратить дальнейшее развитие атаки. Главная сложность при этом заключается в том, чтобы собрать достаточно уникальных индикаторов, которые позволят точно определить тип вредоносного ПО, используемого в каждой конкретной атаке.

Как отмечалось в разделе [Обнаружение \(Identification\)](#), сбор индикаторов компрометации является итерационным процессом, который необходимо повторить несколько раз, для того чтобы быть уверенным в полноте собранных индикаторов.

Для сбора индикаторов компрометации можно воспользоваться описанными ниже инструментами.

### **SYSINTERNALS**

Sysinternals – это набор бесплатных программ для администрирования и мониторинга компьютеров под управлением операционных систем Windows. Пакет Sysinternals Suite включает в себя несколько десятков небольших утилит. Утилиты Sysinternals рекомендуется использовать для сбора первоначальных данных об инциденте.

Наиболее важные утилиты, которые могут быть использованы при реагировании на инциденты, рассмотрены ниже.

Скачать инструменты можно с сайта Microsoft® по ссылке <https://technet.microsoft.com/en-us/sysinternals/default.aspx>.

### **PSTools**

PSTools – набор утилит командной строки для удаленного запуска приложений (PSEXec), получения списка процессов на локальном или удаленном компьютере (PSList), принудительного завершения задач (Pskill), управления службами (PSService). Кроме того, в набор PsTools входят служебные программы для перезагрузки или выключения компьютеров, вывода содержимого журналов событий и многого другого.

## Process Monitor

Process Monitor – программа для наблюдения в реальном времени за действиями различных процессов в среде операционной системы Windows. Утилита включает в себя возможности мониторинга обращений к реестру, обращений к файловой системе и дополнительно позволяет получать более подробную информацию о взаимодействии процессов, использовании ресурсов, сетевой активности и операциях ввода-вывода.

## Process Explorer

Process Explorer – программа для наблюдения в реальном масштабе времени за действиями различных процессов и управления ими в среде операционной системы Windows.

Process Explorer позволяет:

- получать подробную информацию о всех процессах, выполняющихся в среде Windows;
- получать доступ к функциям управления процессами из главного меню или из контекстного меню выбранного процесса;
- использовать функции принудительного завершения (Kill), приостановки (Suspend) и продолжения выполнения (Resume) процессов;
- управлять не только процессами, но и потоками (Threads), а также динамически внедряемыми в основной процесс программными модулями (DLL);
- в любой момент времени принудительно выполнять дампы памяти (Minidump или Fill Dump) с сохранением в выбранный файл.

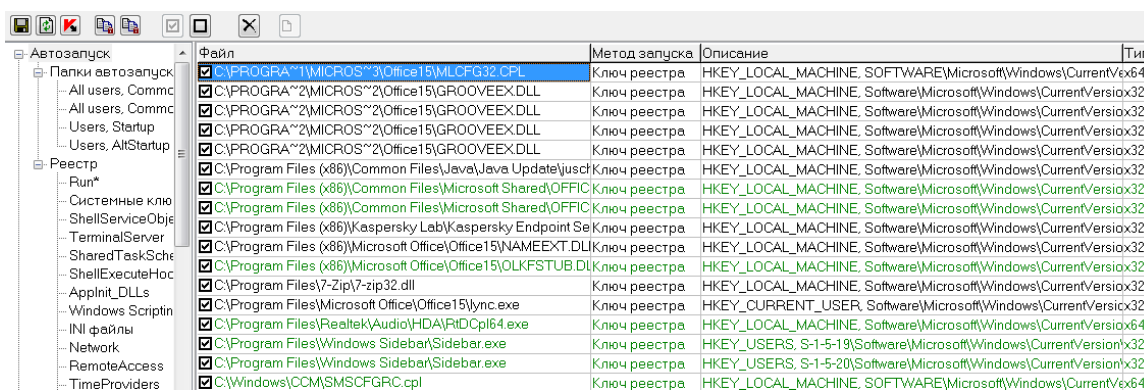
## Autoruns

AutoRuns – утилита для 32 и 64-разрядных ОС Microsoft Windows, которая способна управлять автозагрузкой программ, сервисов, модулей, драйверов и других компонентов системы.

Autoruns отображает все, что будет запущено на компьютере при старте ОС, регистрации пользователя и других событиях. Отображаются программы, загружаемые модули, драйверы, системные службы, назначенные задания, Winlogon. Утилита может показать свойства любого объекта, пути и параметры запуска, а также отменять их автозапуск. Утилита поддерживает возможность проверки файлов автозапуска по хешу на сервисе VirusTotal, при этом неизвестные файлы можно отправить на анализ в антивирусные лаборатории.

## AVZ

Антивирусная утилита AVZ является инструментом для исследования и восстановления системы.



Автозапуск	Файл	Метод запуска	Описание	Тип
Папки автозапуска	<input checked="" type="checkbox"/> C:\PROGRAM~1\MICROS~3\Office15\MLCFG32.CPL	Ключ реестра	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion	64
All users, Commc	<input checked="" type="checkbox"/> C:\PROGRAM~2\MICROS~2\Office15\GROOVEEX.DLL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
All users, Commc	<input checked="" type="checkbox"/> C:\PROGRAM~2\MICROS~2\Office15\GROOVEEX.DLL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Users, Startup	<input checked="" type="checkbox"/> C:\PROGRAM~2\MICROS~2\Office15\GROOVEEX.DLL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Users, AltStartup	<input checked="" type="checkbox"/> C:\PROGRAM~2\MICROS~2\Office15\GROOVEEX.DLL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Реестр	<input checked="" type="checkbox"/> C:\Program Files (x86)\Common Files\Java\Java Update\jusd\	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Рун*	<input checked="" type="checkbox"/> C:\Program Files (x86)\Common Files\Microsoft Shared\OFFIC	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Системные ключи	<input checked="" type="checkbox"/> C:\Program Files (x86)\Common Files\Microsoft Shared\OFFIC	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
ShellServiceObjec	<input checked="" type="checkbox"/> C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Se	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
TerminalServer	<input checked="" type="checkbox"/> C:\Program Files (x86)\Microsoft Office\Office15\NAMEEXT.DLL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
SharedTaskSche	<input checked="" type="checkbox"/> C:\Program Files (x86)\Microsoft Office\Office15\OLKFSTUB.DL	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
ShellExecuteHoc	<input checked="" type="checkbox"/> C:\Program Files\7-Zip\7-zip32.dll	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x32
Applnit_DLLs	<input checked="" type="checkbox"/> C:\Program Files\Microsoft Office\Office15\lync.exe	Ключ реестра	HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion	x32
Windows Scriptin	<input checked="" type="checkbox"/> C:\Program Files\Realtek\Audio\HDA\RtHD Cpl64.exe	Ключ реестра	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion	x64
INI файлы	<input checked="" type="checkbox"/> C:\Program Files\Windows Sidebar\Sidebar.exe	Ключ реестра	HKEY_USERS, S-1-5-19\Software\Microsoft\Windows\CurrentVersion	x32
Network	<input checked="" type="checkbox"/> C:\Program Files\Windows Sidebar\Sidebar.exe	Ключ реестра	HKEY_USERS, S-1-5-20\Software\Microsoft\Windows\CurrentVersion	x32
RemoteAccess	<input checked="" type="checkbox"/> C:\Windows\CCM\SMSCFGRC.cpl	Ключ реестра	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion	64
TimeProviders				

Рисунок 4: Результат работы Менеджера автозапуска AVZ

Утилиту AVZ рекомендуется использовать при расследовании инцидентов в качестве средства получения информации о системе, так как в её состав входят следующие анализирующие систему модули:

- Диспетчер процессов
- Диспетчер служб и драйверов
- Модули пространства ядра
- Менеджер Winsock SPI (LSP, NSP, TSP)
- Открытые порты TCP/UDP
- Менеджер автозапуска
- Менеджер расширений IE
- Менеджер расширений проводника
- Менеджер апплетов панели управления (CPL)
- Менеджер расширений системы печати
- Менеджер планировщика заданий (Task Scheduler)
- Менеджер внедренных dll
- Менеджер протоколов и обработчиков
- Менеджер Active Setup
- Менеджер файла Hosts
- Общие ресурсы и сетевые сеансы

Скачать утилиту можно с сайта <http://www.z-oleg.com/secur/avz/download.php>.

## GMER

Gmer – программный комплекс для обнаружения и удаления руткитов на ОС Microsoft Windows. Поддерживаются 32 и 64-разрядные ОС. Утилита позволяет просканировать компьютер на наличие скрытых процессов, потоков, модулей, файлов, секторов диска, ключей реестра, установленных перехватчиков режима ядра.

Получить подробную информацию о Gmer и скачать утилиту можно по ссылке <http://www.gmer.net/>.

## YARA

YARA – инструмент для помощи исследователям вредоносного ПО в идентификации и классификации вредоносных семплов. Утилита осуществляет сигнатурный анализ на основе формальных YARA-описаний, в которых содержатся индикаторы компрометации для разных типов вредоносного ПО. Каждое описание состоит из набора строк и некоторого логического выражения, по которому определяется логика срабатывания анализатора.

Ниже приведен пример описания, на основе которого YARA определяет объекты, содержащие любой из перечисленных индикаторов (два hex-индикатора и один строковый) как угрозу.

```
rule silent_banker : banker
{
  meta:
    description = "This is just an example"
    thread level = 3
    in the wild = true
  strings:
    $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
    $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
    $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
  condition:
    $a or $b or $c
}
```

Утилита позволяет анализировать как отдельные объекты, так и папки со всеми подпапками, и может использоваться для поиска вредоносного ПО, подпадающего под заданные YARA-описания.

Скачать утилиту можно по ссылке <http://virustotal.github.io/yara/>.

## ИНСТРУМЕНТЫ ДЛЯ СБОРА ДАННЫХ

В данном разделе описаны программы, позволяющие создать дампы оперативной памяти и образы диска.



Размер диска, на который производится запись образа, должен превышать размер диска (или объем памяти), с которого снимается образ, так как при снятии дампа сохраняется не только занятое пространство, а весь образ диска (памяти).

## GRR RAPID RESPONSE

GRR – фреймворк для реагирования на инциденты ИБ. В GRR реализована клиент-серверная архитектура, при которой агенты устанавливаются на машинах пользователей и служат для сбора информации, а сервер предназначен для хранения и анализа собранной информации.

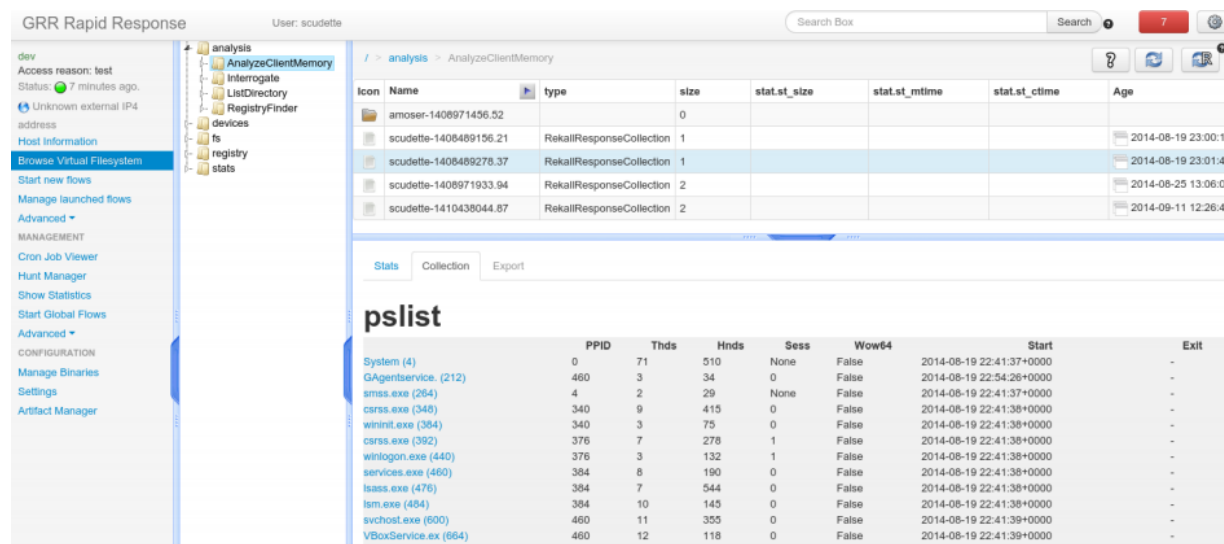


Рисунок 5: Интерфейс программы GRR

Основные возможности:

- удаленный анализ оперативной памяти и реестра Windows (с помощью [Rekall](#)); удаленный анализ диска (с помощью [The Sleuth Kit](#)).

Скачать утилиту GRR и документацию к ней можно по ссылке <https://github.com/google/grr>.

## FORENSIC TOOLKIT

Forensic Toolkit (FTK) – набор утилит для компьютерной криминалистики. В пакет FTK входит утилита FTK Imager. FTK Imager сохраняет образ жесткого диска и позволяет получить дампы памяти.

FTK предусматривает сразу несколько вариантов просмотра образа диска. Например, можно выбрать в меню программы пункт «Электронные таблицы», и FTK выведет список всех найденных xls-файлов с подробным описанием и указанием местоположения. В программе присутствует база ключевых слов, по которым осуществляется поиск компрометирующей информации.

Скачать утилиту можно по ссылке <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk>.

## DD

dd (dataset definition) – утилита UNIX™, предназначенная для копирования и конвертации файлов. Данная утилита позволяет копировать любые секторы жесткого диска, в том числе секторы, которые не используются ОС. Например, dd позволяет создать резервную копию загрузочного

сектора жесткого диска. Для снятия образа диска с использованием dd можно использовать любой дистрибутив Linux. Существуют также версии dd, разработанные под ОС Windows.

## BELKASOFT RAM CAPTURER

Belkasoft RAM Capturer предназначен для помощи в проведении анализа оперативной памяти компьютера. Программа предоставляет возможность снять дамп оперативной памяти компьютера под управлением 32- и 64-разрядных версий Windows, сохранив его в файл для последующего анализа.

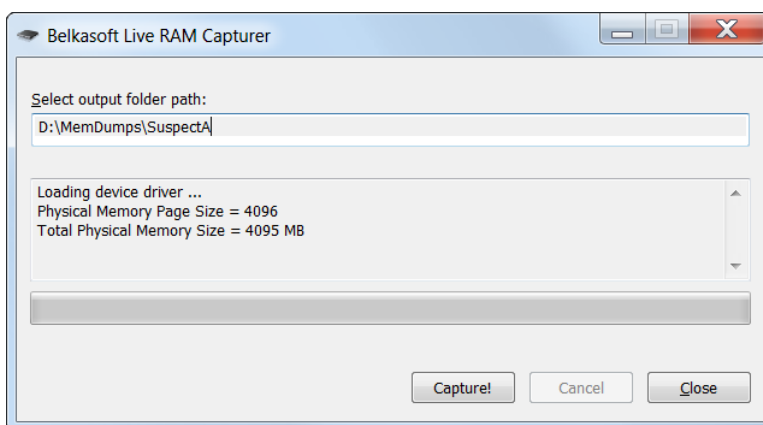


Рисунок 6: Интерфейс программы Belkasoft RAM Capturer

В поставку Belkasoft RAM Capturer входят 32- и 64-разрядные версии драйверов, работающих в режиме ядра и позволяющих корректно обрабатывать области данных, принадлежащие защищенным процессам. Продукт распространяется бесплатно.

Скачать программу можно по ссылке <http://belkasoft.com/ram-capturer>.

## ИНСТРУМЕНТЫ ДЛЯ АНАЛИЗА ПОТЕНЦИАЛЬНЫХ УГРОЗ

Исследование угроз требует большого опыта и постоянной практики в этой области. Для первоначального исследования рекомендуется использовать средства из списка ниже, однако при подозрении на APT-атаку следует доверить исследование угроз экспертам, предоставляющим соответствующие услуги.

### THREAT LOOKUP – KASPERSKY THREAT INTELLIGENCE PORTAL

Решение Kaspersky Threat Lookup позволяет получить информацию по каждому из следующих индикаторов: хеши файлов, URL-, IP-адреса, имя угрозы. При этом результаты поиска будут содержать не только информацию о самом объекте исследования (например, размер для файла, whois-информацию для URL-адреса или географическое положение для IP), но и описания связанных с ним объектов. Например, URL-адреса, с которых был загружен файл, URL-адреса, к которым он обращался.

Информация о связях между индикаторами необходима, так как новые вредоносные программы, которые еще неизвестны, считаются «чистыми» всеми системами обеспечения ИБ. Такое вредоносное ПО можно обнаружить, так как оно может обращаться к URL-адресам, которые известны как источники распространения вредоносного ПО. Это должно сигнализировать исследующему этот файл сотруднику, ответственному за ИБ, о необходимости внимательной проверки файла.

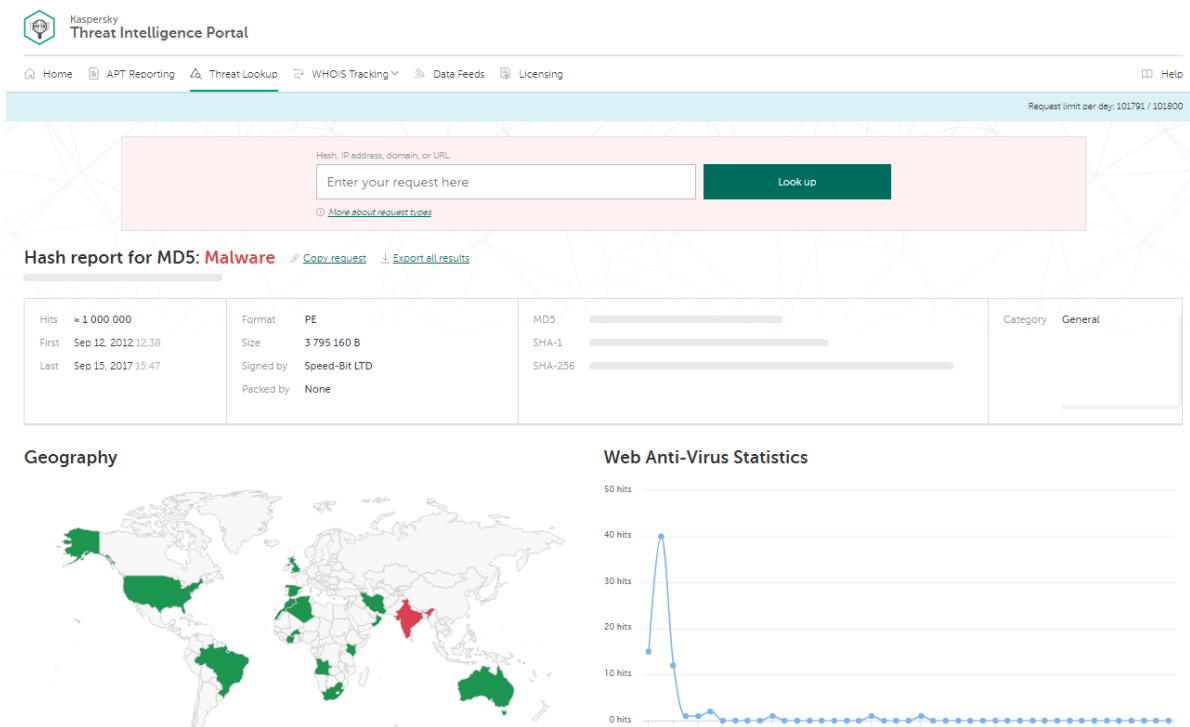


Рисунок 7: Интерфейс решения Threat Lookup

## SANDBOX – KASPERSKY THREAT INTELLIGENCE PORTAL

Одной из возможностей решения Kaspersky Threat Intelligence Portal (TIP) является анализ объекта в Песочнице (Sandbox). В результате эмуляции действий объекта в защищенной среде становится возможным обнаружение ранее неизвестных угроз, а также получение ключевых индикаторов компрометации и подробных отчетов о поведении проанализированного объекта.

Для того чтобы получить результаты анализа объекта в TIP Sandbox, необходимо передать сам объект, ссылку по которой он был загружен, или его хеш-сумму. Кроме отчета о поведении проанализированного объекта, TIP Sandbox предоставляет пользователю набор артефактов, связанных с объектом, в том числе PCAP-файлы с информацией о сетевой активности, файловые объекты, которые были модифицированы анализируемым объектом.

## ИНСТРУМЕНТЫ ДЛЯ АНАЛИЗА ДАМПОВ ПАМЯТИ

### Volatility

Volatility Framework является полностью открытым набором инструментов для извлечения цифровых артефактов из оперативной памяти.

Volatility позволяет работать со следующими типами дампов:

- Raw/Padded Physical Memory;
- Firewire® (IEEE 1394);
- Expert Witness (EWF);
- 32- and 64-bit Windows Crash Dump;
- 32- and 64-bit Windows Hibernation;
- 32- and 64-bit MachO files;
- Virtualbox Core Dumps;
- VMware™ Saved State (.vmss) and Snapshot (.vmsn);
- HPAK Format (FastDump);
- LiME (Linux Memory Extractor);

- QEMU VM memory dumps.

В стандартной поставке Volatility более 150 плагинов. Используя различные плагины Volatility, можно получить информацию о дереве вызова процессов и загруженных в процессы библиотеках, а также другие данные. Например, с помощью плагина DeviceTree можно получить список всех устройств и подключенных к ним драйверов системы. Такой список можно использовать для поиска драйверов, встроенных руткитами.

Утилита поддерживает обработку дампов памяти с ОС Linux®, Windows и Mac® OS X® с помощью соответствующих профилей (более 30 штук, для всех Windows OS от Windows XP и старше).

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP2x86 dlldump -memory -D stuxout/
Volatility Foundation Volatility Framework 2.5
Process(V) Name           Module Base Module Name  Result
-----
0x820df020 smss.exe      0x048580000 smss.exe      OK: module.376.22df020.48580000.dll
0x821a2da0 csrss.exe     0x075b40000 CSRSRV.dll   OK: module.600.23a2da0.75b40000.dll
0x821a2da0 csrss.exe     0x077f10000 GDI32.dll    Error: DllBase is paged
0x821a2da0 csrss.exe     0x075b60000 winsrv.dll  OK: module.600.23a2da0.75b60000.dll
0x81da5650 winlogon.exe 0x001000000 winlogon.exe OK: module.624.1fa5650.1000000.dll
```

Volatility имеет режим сохранения отдельных процессов в виде исполняемых файлов, которые можно подвергнуть статическому и динамическому анализу с помощью различных средств, например, [Strings](#) или [Sandbox – Kaspersky Threat Intelligence Portal](#).

В интернете можно найти множество учебных дампов для анализа с помощью Volatility и документацию к фреймворку.

Скачать программу можно по ссылке <http://www.volatilityfoundation.org/>.

## Rekall

Rekall – фреймворк и набор утилит для анализа памяти.

Rekall предоставляет пользователям три интерфейса: интерфейс командной строки, интерфейс интерактивной консоли на основе IPython и web-консоль. Как и Volatility, Rekall располагает большим количеством плагинов, например, плагин pslist позволяет вывести список всех процессов, которые были запущены в системе, а плагин hooks\_inline позволяет найти все библиотеки с установленными перехватами.

```
user@computer:~/rekall$ rekall -f ~/images/win7.elf
-----
The Rekall
Memory Forensic framework 1.1.0 beta (Buchenegg).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.
-----
win7.elf 12 47 07> pslist
-----> pslist()
  _EPROCESS      Name           PIO PPID Thds Hnds Sess Wow64 Start
-----
0xfa80008959e0 System 4           0 84 511 -      False 2012-10-01 21:39:51+0000
[1] zeus.vmem 00:10:03> hooks inline proc regex="services"
-----> hooks_inline(proc_regex="services")
Pid Proc         DLL           Name           Hook           Disassembly
-----
676 services.exe ntdll.dll     NtCreateThread 0x7e3b47       0x7c90d7d2 e97063ed83     jmp 0x7e3b47 (vad_0x7e0000+0x3b47)
                                0x7c90d7d7 ba0003fe7f     mov edx, 0x7ffe0300
                                0x7c90d7dc ff12          call dword ptr [edx]
                                0x7c90d7de c22000       ret 0x20
                                0x7c90d7e1 90           nop
                                0x7c90d7e6 90           nop
                                0x7c90d7e7 b836000000   mov eax, 0x36
```

Для снятия дампа памяти на ОС Windows в составе пакета Rekalл есть утилита winpmem. Rekalл позволяет анализировать не только файл дампа памяти, но и память на работающей машине. То есть с помощью Rekalл можно проводить анализ оперативной памяти без снятия дампа.

Скачать программу можно по ссылке <http://www.rekalл-forensic.com/>.

## ИНСТРУМЕНТЫ ДЛЯ АНАЛИЗА ОБРАЗОВ ДИСКА

### The Sleuth Kit

The Sleuth Kit (TSK) представляет собой библиотеку и набор инструментов командной строки, которые позволяют исследовать образы дисков, а также анализировать данные о файловой системе и содержимое файлов.

Утилиты в пакете TSK предоставляют возможности для считывания и анализа данных, содержащихся на диске, отображения структуры метаданных, определенной в файловых системах. В этой структуре метаданных хранится метаинформация о стандартных файлах, каталогах или других объектах файловой системы. Утилиты TSK обращаются к диску в обход файловой системы, используя собственные драйверы, и позволяют находить удаленные или скрывающиеся файловые объекты.

Скачать пакет можно по ссылке <http://www.sleuthkit.org/sleuthkit/>.

### Autopsy

Autopsy является удобной оболочкой к набору консольных утилит [The Sleuth Kit](#) (TSK). Autopsy – это приложение, запускающее приложения из набора TSK и обрабатывающее (визуализирующее) их вывод. Приложение позволяет анализировать содержимое жесткого диска на работающих системах (работать с дисками напрямую), либо из образов (например, снятых при помощи утилит, подобных DD).

Скачать оболочку можно по ссылке <http://www.sleuthkit.org/autopsy/>.

### RegRipper

RegRipper – это написанная на Perl утилита, позволяющая извлекать и анализировать значения ветвей реестра Windows с возможностью сохранить полученную информацию в файл отчета. Утилита предназначена для работы с образами дисков, а не с «живой» системой. Для доступа к реестру RegRipper не использует Win32API. Для работы с программой можно использовать графический интерфейс или утилиту командной строки.

```
C:\RR>rip.exe
Rip v.2.8_20130801 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

-r Reg hive file...Registry hive file to parse
-g .....Guess the hive file (experimental)
-f [profile].....use the plugin file (default: plugins\plugins)
-p plugin module...use only this module
-l .....list all plugins
-c .....Output list in CSV format (use with -l)
-s system name....Server name (TLN support)
-u username.....User name (TLN support)
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -l -c
```

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

Стандартный дистрибутив содержит более 300 различных плагинов. Скачать RegRipper можно по ссылке <https://github.com/keydet89/RegRipper2.8>.

## STRINGS

Strings – стандартная утилита UNIX-подобных ОС, применяемая для поиска печатаемых строк, которые могут служить дополнительными индикаторами. Она выводит последовательности печатаемых символов, обнаруженных в заданном файле. Может использоваться для визуального анализа дампов-файлов (core dump) или для поиска информации о ПО, используемом при разработке угрозы, URL-, IP-адресах, с которыми может взаимодействовать файл, ключей реестра, к которым он может обращаться, адресов электронной почты и иных индикаторов.

В рамках пакета Cygwin утилита Strings портирована на Microsoft Windows. Скачать пакет можно по ссылке <https://cygwin.com/>.

## ИНСТРУМЕНТЫ ДЛЯ УДАЛЕНИЯ УГРОЗ

### KASPERSKY VIRUS REMOVAL TOOL

Kaspersky Virus Removal Tool — бесплатная программа для проверки и лечения зараженных компьютеров под управлением операционных систем Windows.

Утилита не предназначена для постоянной защиты компьютера. По окончании лечения компьютера программу следует удалить и заменить полноценным антивирусом. В программе Kaspersky Virus Removal Tool отсутствует функция обновления баз. Чтобы получить программу с актуальным набором баз, ее необходимо каждый раз загружать с серверов «Лаборатории Касперского».

Основные возможности Kaspersky Virus Removal Tool:

- Обнаружение и удаление вредоносного ПО.

Обнаружение Adware и легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

- Резервное копирование файлов перед лечением/удалением.
- Защита от удаления системных файлов.
- Предотвращение ложных срабатываний.

Запуск с использованием командной строки.

Скачать Kaspersky Virus Removal Tool можно с сайта «Лаборатории Касперского» по ссылке <http://www.kaspersky.ru/antivirus-removal-tool>.

Другие бесплатные утилиты «Лаборатории Касперского» для удаления отдельных видов вредоносного ПО можно найти на сайте Технической поддержки <http://support.kaspersky.com/viruses/utility?CID=acq-freekasp-USA&qa=1.198229483.571661967.1434556259>.

### KASPERSKY RESCUE DISK

Kaspersky Rescue Disk применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения (например, Kaspersky Virus Removal Tool), запускаемых под управлением операционной системы.

При этом эффективность лечения повышается за счет того, что находящиеся в системе вредоносные программы не получают управления во время загрузки операционной системы. В режиме аварийного восстановления доступны только задачи проверки объектов и обновления баз, а также откат обновлений и просмотр статистики.

Скачать Kaspersky Rescue Disk можно с сайта «Лаборатории Касперского» по ссылке <https://support.kaspersky.ru/viruses/rescuedisk>.

## **СПЕЦИАЛЬНЫЕ РЕШЕНИЯ ЛАБОРАТОРИИ КАСПЕРСКОГО**

### **АНАЛИТИЧЕСКИЕ ОТЧЕТЫ ЛАБОРАТОРИИ КАСПЕРСКОГО ОБ УГРОЗАХ КЛАССА АРТ**

Аналитические отчеты об угрозах класса АРТ позволяют применять проактивный подход к защите, благодаря эксклюзивному доступу к подробным описаниям крупных компаний кибершпионажа. Подписка на отчеты включает в том числе доступ к соответствующим индикаторам компрометации (indicators of compromise, IOC) в YARA и OpenIOC форматах. За последнее время было опубликовано более 60 подробных отчетов об АРТ-угрозах.

Примеры отчетов можно найти на портале <https://tip.kaspersky.com/AptReporting>.

# ПРИМЕР РЕАГИРОВАНИЯ НА ИНЦИДЕНТ ИБ

В этом разделе рассмотрен возможный сценарий целевой атаки, а также показаны действия, которые должны будут провести сотрудники, ответственные за ИБ атакуемой организации.

## АТАКА

Ниже описан план атаки, который мог бы быть разработан злоумышленниками. В квадратных скобках обозначены порядковые номера шагов – далее они будут использоваться в качестве ссылок при реагировании на атаку.

- [Шаг 1] Планируется атака на банк с целью получения доступа к системе управления банкоматами для хищения денег. После выбора банков для атаки злоумышленник использует методы разведки и социальную инженерию для определения способа проникновения в компьютерную сеть банка.
- [Шаг 2] В результате злоумышленник решает отправить нескольким сотрудникам банков сообщения электронной почты (spear phishing) от имени финансового регулятора – Центрального банка Российской Федерации (Банк России). Эти сообщения будут содержать вложенный pdf-документ, использующий уязвимости Adobe® Reader для загрузки на компьютер жертвы других инструментов атаки (payload).

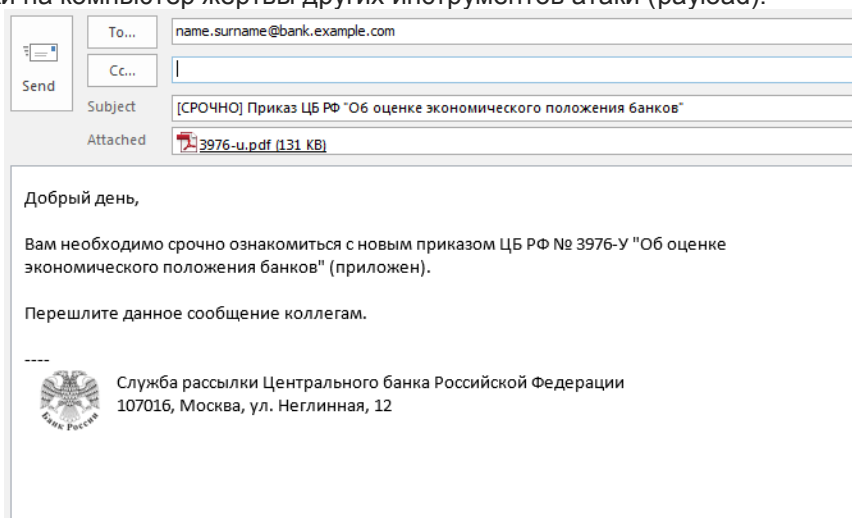


Рисунок 8: Пример использования spear-phishing через сообщение электронной почты

- [Шаг 3] После того, как жертва получит письмо и попытается открыть pdf-файл, на ее компьютер будет установлено приложение-загрузчик. Это приложение пропишет себя в автозагрузку и при следующем включении компьютера загрузит с сервера злоумышленника программу-бота, которая обеспечит злоумышленнику возможность исполнять команды на компьютере жертвы.
- [Шаг 4] Приложение-загрузчик добавит программу-бота в автозапуск. При этом приложение-загрузчик не удалит себя из списка автозагрузки, чтобы при следующих запусках проверять наличие на компьютере программы-бота. В случае, если программа-бот не будет обнаружена, приложение-загрузчик повторно загрузит его.



[Шаг 5]

Программа-бот после запуска будет постоянно присутствовать в памяти компьютера. Чтобы не вызывать подозрений у пользователя, в списке запущенных процессов она будет маскироваться под известное приложение `lsass.exe` (Local Security Authentication Server), которое всегда запущено на всех Windows-компьютерах.

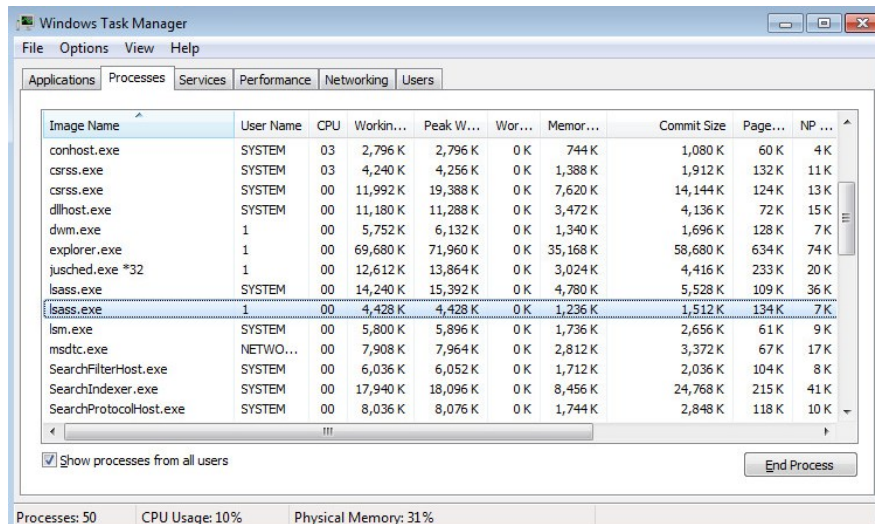


Рисунок 9: Обычно `lsass.exe` должен быть запущен в одном экземпляре от имени операционной системы. Например, *Stuxnet* использовал фальшивый `lsass`, чтобы скрыть своё присутствие в системе.

[Шаг 6]

Для получения команд бот будет периодически обращаться к серверу управления (C&C), подконтрольному злоумышленнику.

[Шаг 7]

При первом обращении бот получит команду на дальнейшее распространение по сети (Lateral movement). Для этого он попытается подключиться к другим компьютерам в сети.

[Шаг 8]

Как только бот обнаружит машину, на которой производился вход от имени Администратора, он обратится на C&C для загрузки программы `Mimikatz` и средства удаленного администрирования `Ammy Admin`. Программа `Mimikatz` позволит злоумышленнику получить в открытом виде пароли всех пользователей, которые вводили свои логин и пароль.

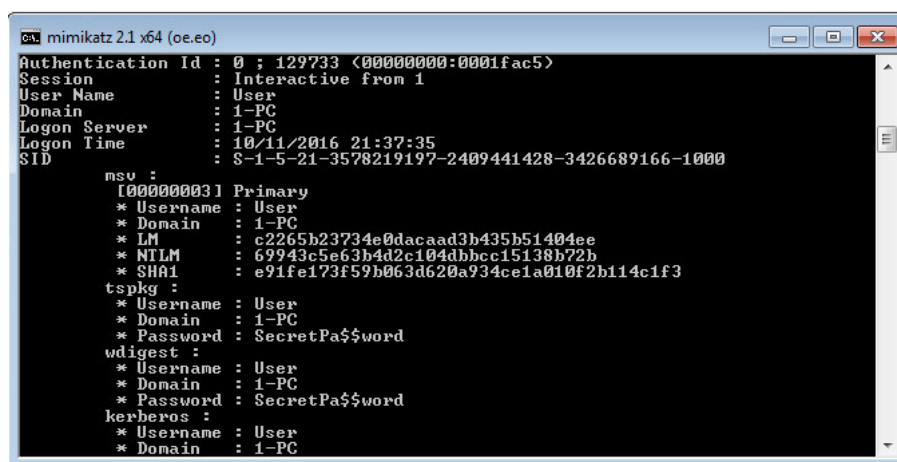


Рисунок 10: Пример выполнения программы `Mimikatz`. В открытом виде выводятся все логины и пароли, в том числе пароли пользователей `Active Directory`®.

[Шаг 9]

В случае успеха бот сможет подключиться к ATM Gateway и произвести атаку на банкоматы. Например, злоумышленник может внедрить в банкоматы программу, которая будет выдавать деньги при обнаружении специальной пластиковой карты. Если цель атаки будет достигнута, сервер управления отправит ботам команду на удаление следов заражения. После получения такой команды бот предпримет все возможные действия, для того чтобы скрыть факт заражения и помешать возможному расследованию.

Далее будут рассмотрены способы помешать достижению целей атаки.

## РЕАГИРОВАНИЕ

### ОПИСАНИЕ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Как отмечалось выше, реагирование на угрозы начинается с подготовки (теоретическое описание этапа см. в разделе [Подготовка](#)).

В данном случае атакуемая организация была готова к атакам:

- Банк использует SIEM-систему IBM QRadar®, в которую интегрированы потоки данных об угрозах, собранные специалистами «Лаборатории Касперского».
- Для доступа в интернет все сотрудники используют прокси-сервер Squid, отправляющий информацию о сетевых соединениях в SIEM.
- Для работы с электронной почтой используется MTA Postfix, который также отправляет в SIEM события о проходящих через него письмах. Отправляемые MTA события расширены информацией из заголовков (headers) письма, содержащей, например, все записи Received, данные о подписи DKIM-Signature и другую информацию.
- На всех рабочих станциях Банка установлен антивирус Kaspersky Endpoint Security, который централизованно управляется с помощью Kaspersky Security Center. Вся информация о срабатываниях антивируса на любом компьютере также попадает в SIEM.
- Для маршрутизации сетевых пакетов в инфраструктуре Банк применяет компьютер на базе ОС Linux. Банкоматы отделены от основной сети банка, доступ в сеть банкоматов разрешен только некоторым пользователям.
- Кроме того, Банк имеет активную подписку на решение [Threat Lookup – Kaspersky Threat Intelligence Portal](#).

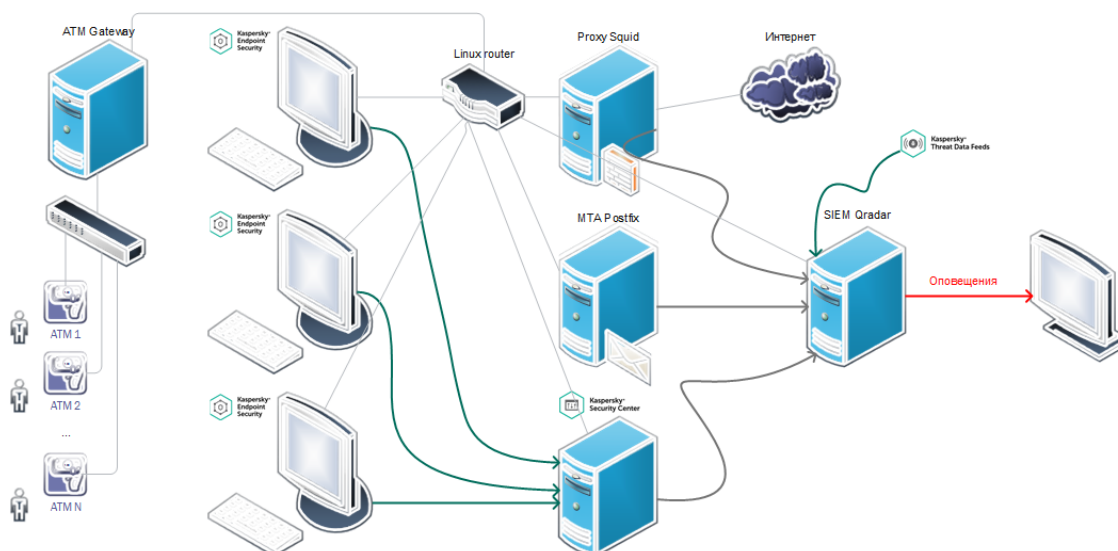


Рисунок 11: Общая схема корпоративной сети Банка

## ОБНАРУЖЕНИЕ АТАКИ

Благодаря тому, что все запрашиваемые URL- и IP -адреса сопоставляются с потоками данных об угрозах, возможно достоверное обнаружение атаки на ранних этапах:

1. IP-адрес сервера, отправившего сообщение электронной почты будет детектирован в SIEM по IP Reputation Data Feed [Шаг 2].
2. Запрос на загрузку бота будет детектирован в SIEM по Malicious URL Data Feed [Шаг 3].
3. Обращение к серверу управления (C&C) будет детектировано в SIEM по Botnet C&C URL Data Feed [Шаг 6].
4. Mimikatz будет обнаружен и удален Endpoint-антивирусом KES, информация об обнаружении попадет в SIEM [Шаг 8].

Как отмечалось выше, чем раньше атака будет обнаружена, тем меньший ущерб будет нанесен атакуемой организации. Предположим, что из-за высокой загруженности сотрудник, отвечающий за ИБ, не смог отреагировать на первые оповещения, и к моменту начала реагирования атака успела дойти до шестого шага (см. [Шаг 6]).

Таким образом, предположим, что этап обнаружения начался с оповещения об обращении на Botnet C&C URL, пришедшего в SIEM.

Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:22:0...	Botnet Address	10.65.65.65
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:21:5...	Botnet Address	10.65.65.65

Рисунок 12: События об обнаружении BotnetCnC-адресов с помощью Kaspersky Threat Feed Service в интерфейсе SIEM QRadar

## РЕАГИРОВАНИЕ НА АТАКУ

### Сдерживание

Обращение к серверам управления свидетельствует о наличии активного заражения. Поэтому необходимо как можно скорее определить зараженные компьютеры и ограничить для них доступ к внутренней и внешней сети (например, заблокировать пересылку пакетов с помощью iptables).

Для того чтобы локализовать заражение, требуется найти в SIEM-системе все обращения к обнаруженному Botnet C&C URL. Все компьютеры, которые были выявлены таким способом, заражены, и их необходимо изолировать. Дополнительно следует исследовать обнаруженный Botnet C&C URL с помощью решения [Threat Lookup](#) – Kaspersky Threat Intelligence Portal. В результате исследования необходимо получить хеши программ-ботов, которые взаимодействовали с этим C&C URL, а также все URL, с которыми взаимодействовали найденные программы-боты. После этого нужно повторить поиск в SIEM по расширенному списку индикаторов, так как один и тот же бот мог взаимодействовать с несколькими C&C URL на разных компьютерах.

Следующая команда, выполненная на компьютере, выполняющем роль маршрутизатора, запретит пересылать пакеты на адрес 192.168.0.3. Это лишит вредоносное ПО возможности распространяться по сети или отправлять данные через интернет.

```
iptables -A FORWARD -s 192.168.0.3 -j DROP
```

Далее следует проанализировать записи в SIEM, связанные с скомпрометированной машиной (или машинами, если обнаружилось несколько зараженных компьютеров). В результате анализа будет обнаружено, что первым событием в цепочке было детектирование Spam IP-адреса, который был бы детектирован на [Шаг 3] (нижнее событие на скриншоте – KL\_IP\_Reputation). Это значит, что компрометация началась с получения письма по электронной почте. Необходимо выяснить, получал ли кто-то ещё подобные сообщения, и исследовать машины этих пользователей аналогично описанному выше алгоритму.

Event Name	Log Source
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
KL_Malicious_URL	KL_Threat_Feed_Service_v2
KL_Malicious_URL	KL_Threat_Feed_Service_v2
KL_IP_Reputation	KL_Threat_Feed_Service_v2

Рисунок 13: Результаты поиска всех детектирующих событий от Kaspersky Threat Feed Service в интерфейсе SIEM QRadar

Также, рекомендуется сразу, не дожидаясь итогов расследования, добавить в черные списки обнаруженный C&C URL, так как наличие этого URL в потоках данных об угрозах, собранных специалистами «Лаборатории Касперского», означает наличие зараженных пользователей, уже взаимодействовавших с этим C&C URL.

## Выявление вредоносного ПО

После того, как зараженные машины были изолированы (например, с помощью `iptables`), можно приступить к поиску процесса, инициировавшего обращения на C&C URL. В простейшем случае после поиска по решению [Threat Lookup](#) – Kaspersky Threat Intelligence Portal можно получить описание программы-бота и просканировать компьютер на наличие файлов, соответствующих полученному описанию. Это можно сделать, например, по имени, хешу или местоположению файла. Рассмотрим более сложный случай, когда поиск по URL не дал достаточного количества информации. Это значит, что нужно переходить к исследованию зараженной машины.

В случае, если бы соединение все еще было активно, выявить процесс было бы легко с помощью утилиты `netstat`. Но в большинстве случаев соединение уже разорвано, и не существует универсального способа установить инициировавший соединение процесс. Информация о разорванном соединении может некоторое время оставаться в оперативной памяти, и ее можно извлечь с помощью средств анализа дампов памяти. В данном случае программу-бота можно обнаружить с помощью анализа автозагрузки ([Autoruns](#)) и с помощью анализа содержимого оперативной памяти ([Volatility](#)).

Произведем запуск Autoruns непосредственно на зараженной машине.

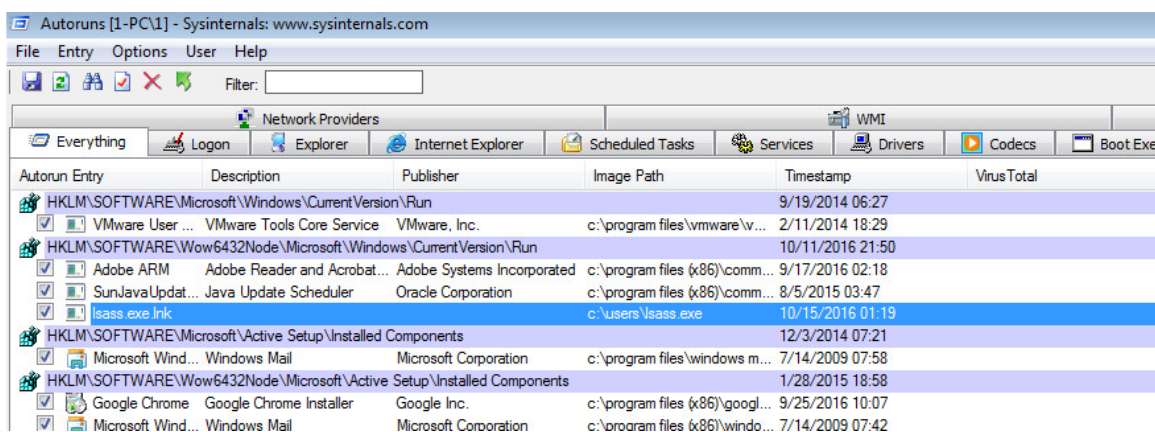


Рисунок 14: Анализ объектов автозапуска с помощью программы Autoruns

В результате может быть обнаружен подозрительный файл `Isass.exe`, так как наличие команды запуска этого приложения в данном ключе реестра не является типичной конфигурацией рабочей станции.

Этот же файл можно обнаружить с помощью снятия и анализа дампа памяти. Для того чтобы снять дамп памяти, используем, например, [Forensic Toolkit](#).

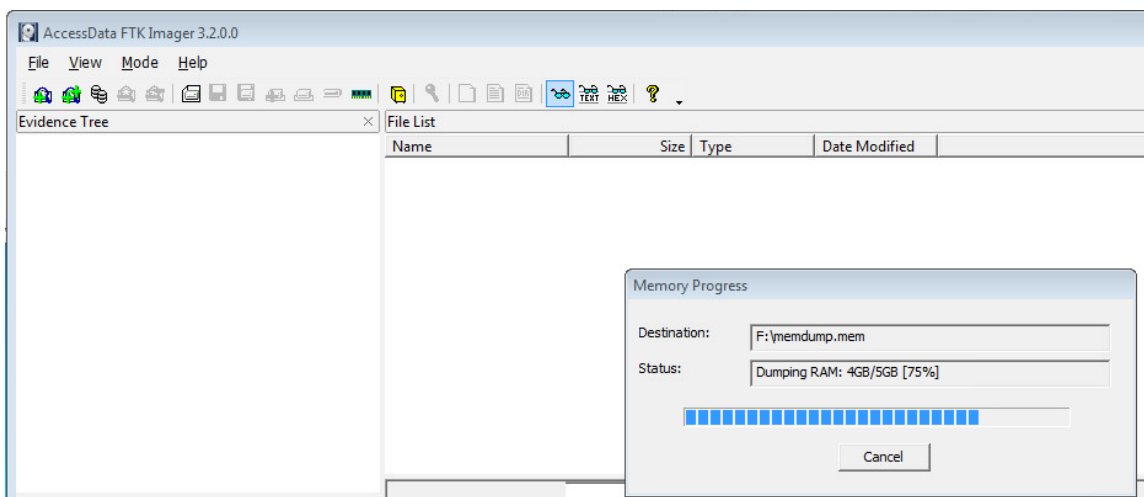


Рисунок 15: Снятие дампа памяти с помощью утилиты FTK Imager

Далее при помощи Volatility получим список процессов, запущенных на зараженном компьютере на момент снятия дампа (фрагмент).

```
C:\Users\User>volatility 2.5>volatility.exe pslist -f C:\Users\User\Memdump\1-PC.mem --profile=Win7SP0x64
Volatility Foundation Volatility Framework 2.5
Offset (V)      Name                PID  PPID  Thds   Hnds   Sess  Wow64  Start
-----
0xfffffa8003c6c890 System              4    0     96   2276  -----  0  2016-10-14 18:01:56 UTC+0000
0xfffffa8004400950 smss.exe           264   4      2     29  -----  0  2016-10-14 18:01:56 UTC+0000
0xfffffa80048e3b30 csrss.exe          352  344    9    620    0  0  2016-10-14 18:02:03 UTC+0000
0xfffffa8004b57420 wininit.exe       404  344    3     76    0  0  2016-10-14 18:02:04 UTC+0000
0xfffffa8004b45b30 csrss.exe          412  396   10    280    1  0  2016-10-14 18:02:04 UTC+0000
0xfffffa8004b7a6a0 winlogon.exe       448  396    3    108    1  0  2016-10-14 18:02:04 UTC+0000
0xfffffa8004bcc2e0 services.exe      508  404    7    224    0  0  2016-10-14 18:02:05 UTC+0000
0xfffffa8004ca9b30 lsass.exe        516   404    8    847    0  0  2016-10-14 18:02:05 UTC+0000
0xfffffa8004cadb30 lsm.exe           524  404   10    189    0  0  2016-10-14 18:02:05 UTC+0000
0xfffffa8005b37660 explorer.exe    1976 1916   33    992    1  0  2016-10-14 18:02:39 UTC+0000
0xfffffa8005ce4b30 lsass.exe      2336 1976   10    231    1  1  2016-10-14 18:02:45 UTC+0000
0xfffffa8005ceab30 svchost.exe       2348 508   14    334    0  0  2016-10-14 18:02:45 UTC+0000
```

В системе присутствуют два процесса lsass.exe, хотя должен быть только один. Если проанализировать, кто запускал каждый из этих процессов, то можно заметить, что lsass.exe с PID 516 был запущен процессом wininit.exe, а второй lsass.exe с PID 1976 был запущен процессом explorer.exe. Обычно lsass.exe запускает именно wininit.exe. Следовательно, процесс с PID 1976 является подозрительным.

Необходимо убедиться, что именно выявленное приложение обращалось к серверу управления. Для этого приложение подвергается исследованию с помощью статического или динамического анализа. Например, с помощью утилиты [Strings](#) можно обнаружить искомый C&C URL.

Утилита имеет несколько важных параметров, в том числе длину минимальной последовательности символов или размер символа (например, 1 байт, 2 байта, 4 байта). Если использовать параметры по умолчанию, можно получить подобный вывод (фрагмент):

```
$ strings -a 'lsass.exe'
f:\dd\vctools\cert\crtw32\dllstuff\atonexit.c
>"g/
BSJB
v4.0.30319
#Strings
#GUID
#Blob
~,#
```

При исследовании можно менять размеры кодировки искомых символов. Это делается для того, чтобы обнаруживать строки, сохраненные в разных кодировках. Например, в режиме отображения шестнадцатитбитных символов будет получен такой результат (фрагмент):

```
$ strings -a -e l 'lsass.exe'
*.msg
Administrator
  native startup state ==  initialized
  _controlfp_s(((void *)0), 0x00010000, 0x00030000)
http://subbotnet-domain_19.botnet-domain.com/page/c
find_proxy
{0}: {1}
--- Start of primary exception ---
```

В примере выше жирным шрифтом выделены строки, которые должны привлечь внимание сотрудника, ответственного за ИБ. В исходном коде обнаружен C&C URL. Это значит, что выявлена именно та программа, которая обращалась к C&C. Также подозрительной является строка с именем пользователя Administrator.

После того, как программа-бот установлена, необходимо передать ее для исследования в антивирусную компанию. Это обеспечит оперативный выпуск обновления антивирусных баз. Это обновление антивирусных баз в дальнейшем можно будет применить на других компьютерах сети, на которых установлен антивирус.

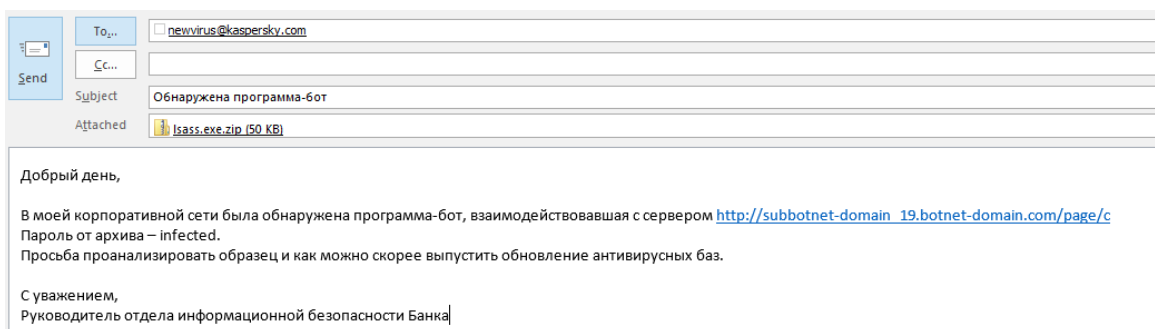


Рисунок 16: Передача обнаруженной программы-бота в антивирусную компанию

Также на этом этапе следует исследовать машину на наличие иного вредоносного ПО и установить, как оно попало на компьютер. По событиям в SIEM было определено, что атака началась с письма по электронной почте. Письмо следует попытаться найти, а вложения из него проанализировать. Для такого анализа можно использовать [Sandbox](#) – Kaspersky Threat Intelligence Portal или специальную виртуальную машину, которая не имеет доступа к внутренней сети, а весь трафик с внешней сетью перехватывается (например, с помощью tcpdump). Благодаря подобному подходу, удастся установить поведение, описанное на [\[Шаг 3\]](#). Если же аналогично проанализировать программу-бота, можно будет установить попытку скачивания Mimikatz (см. [\[Шаг 8\]](#)). Следует проанализировать наличие на зараженных компьютерах полученного образца Mimikatz, так как отсутствие обнаружения этой программы Endpoint-антивирусом не является гарантией отсутствия на компьютере модификации этой программы.

Таким образом, была восстановлена картина атаки:

1. Spear-phishing письмо содержало pdf-файл, при открытии которого скачивалась программа-загрузчик.
2. Программа-загрузчик устанавливала программу-бота.
3. Программа-бот не успела распространиться в сети, но успела закрепиться на одном компьютере и обращалась за командами к серверу управления.
4. Так как на компьютере с ботом не было активного аккаунта Администратора, Mimikatz не был загружен, атаку удалось прервать.

Так как атака была вовремя обнаружена, удалось избежать серьезного ущерба, и банк решил не привлекать к расследованию правоохранительные органы. В таком случае можно переходить к удалению всех обнаруженных вредоносных программ.

## Удаление

Для полного удаления вредоносного ПО необходимо не только удалить с компьютеров обнаруженные в процессе расследования угрозы, но и запустить полное антивирусное сканирование с удалением всех обнаруженных объектов.

## Выводы

Информация по инциденту объединяется в отчет. Все обнаруженные в процессе реагирования индикаторы (в том числе связанные с ними Email-, URL-адреса или хеши) должны быть внесены в черные списки устройств, обеспечивающих ИБ. Все собранные образцы следует отправить в антивирусные компании. Кроме того, для сотрудников должен быть проведен повторный инструктаж о правилах работы с электронной почтой.

# АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

**Продукты.** Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

**Технологии.** Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

**Достижения.** За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.



# УВЕДОМЛЕНИЕ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

FireWire, Mac, Mac OS и OS X – товарные знаки Apple Inc., зарегистрированные в США и других странах.

IBM, QRadar – товарные знаки IBM, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Active Directory, Microsoft, Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

VMware – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Tor – товарный знак The Tor Project, регистрация в США № 3 465 432.

Virtualbox – зарегистрированный товарный знак Oracle Corporation и / или ее аффилированных компаний.

Belkasoft – зарегистрированный в США товарный знак Юрия Губанова.