|  |  |
| --- | --- |
| *voenmeh* | МИНОБРНАУКИ РОССИИ  федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»**  **(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова»)** |
| БГТУ.СМК-Ф-4.2-К5-01 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Факультет |  | И | |  |  | Информационные и управляющие системы |
|  |  | шифр | |  |  | наименование |
| Кафедра |  | И9 | |  |  | Систем управления и компьютерных технологий |
|  |  | шифр | |  |  | наименование |
|  |  |  |  | | | |

|  |
| --- |
| КУРСОВАЯ РАБОТА  на тему |
| Исследование проблем информационной безопасности |
| в Сети Интернет |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент группы | | | |  | | И9М31 |
| Загута Д.В. | | | | | | |
| Фамилия И.О. | | | | | | |
| **РУКОВОДИТЕЛЬ** | | | | | | |
| Романов Л.С. | |  |  | | | |
| Фамилия И.О. Подпись | | | | | | |
| Оценка |  | | | |  | |
| «\_\_\_\_\_» |  | | | | 2018 г. | |

САНКТ-ПЕТЕРБУРГ

2018 г.

**СОДЕРЖАНИЕ**

[ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc523929146)

[ВВЕДЕНИЕ 4](#_Toc523929147)

[1 целевыЕ атакИ 5](#_Toc523929148)

[1.1 Диверсии и саботаж выходят на передний план 9](#_Toc523929149)

[1.2 Финансовые кражи: злоумышленники теперь нацелены на большие суммы 12](#_Toc523929150)

[1.3 Экономический шпионаж 13](#_Toc523929151)

[1.4 Подрывная деятельность как новый объект целенаправленных атак 15](#_Toc523929152)

[2 Тактики целевых атак 19](#_Toc523929153)

[2.1 Уязвимости нулевого дня 19](#_Toc523929156)

[2.2 Living off the land 20](#_Toc523929157)

[2.2.1 Как группа Timberworm использовала тактику "жить за счет земли" 21](#_Toc523929158)

[2.2.2 Инструменты, используемые злоумышленниками 23](#_Toc523929159)

[2.3 Электронная почта как предпочтительный канал для атаки 25](#_Toc523929160)

[2.3.1 Вредоносные программы 26](#_Toc523929161)

[2.3.2 Фишинг 30](#_Toc523929162)

[2.3.3 Программы-вымогатели 33](#_Toc523929163)

[2.3.4 Интернет вещей (IoT) и облачные технологии 33](#_Toc523929164)

[2.4 Появление новых угроз 34](#_Toc523929165)

[ЗАКЛЮЧЕНИЕ 36](#_Toc523929166)

[Список использованных источников 39](#_Toc523929167)

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

|  |  |  |
| --- | --- | --- |
| ПО | — | Программное Обеспечение; |
| DDoS | — | Distributed Denial of Service; |
| IoT | — | Internet of Things; |
| APT | — | Advanced Persistent Threat; |
| БД | — | База Данных; |
| АСУ | — | Автоматизированная Система Управления; |
| САПР | — | Cистема Автоматизированного Проектирования; |

# ВВЕДЕНИЕ

Интернет — глобальная компьютерная сеть, охватывающая весь мир, количество пользователей которой уже превысило 4 миллиарда. В связи с этим на сегодняшний день можно отметить большое число слабо подготовленных пользователей в области информационных технологий, которые имеют весьма смутное представление о потенциальных угрозах, которые могут подстерегать их в сети. В результате их компьютеры оказываются заражёнными разнообразным вредоносным и нежелательным программным обеспечением, которое занимается кражей персональной информации, ученых данных и данных платежных систем, участвует в распределённых DDoS атаках, используются спамерами для организации массовых рассылок, и прочее.

Кибер - атаки последних лет выявили новый масштаб амбиций злоумышленников. Это и многомиллионные ограбления банков, неприкрытые попытки сорвать в США ход избирательного процесса со стороны хакерских групп, а так же крупнейшие распределенные атаки типа «Отказ от обслуживания» (DDoS) ботнетом, созданным из зараженных устройств «интернета вещей» (IoT)

Не смотря на то, что кибер - атаки смогли вызвать беспрецедентные уровни сбоев, нападавшие часто использовали очень простые инструменты и тактику, имеющих наибольшее воздействие. Уязвимости нулевого дня и сложные вредоносные программы в настоящее время, как правило, используются мало. Злоумышленники все чаще полагаются на простые подходы, такие как фишинг - письма и технологию “living off the land” (дословный перевод «жить за счет земли»), используя при этом любые подручные инструменты, такие как легальное программное обеспечение для сетевого администрирования и особенности операционных систем [1].

Например, Mirai — ботнет, стоящий за волной крупных DDoS атак, в основном состоял из зараженных маломощных и плохо защищенных камер видеонаблюдения. В руках злоумышленников даже относительно безобидные устройства и программное обеспечение может быть использовано в разрушительных целях.

В данной работе будут рассмотрены и проанализированы целевые атаки, как представляющие наибольшую угрозу для корпоративного и государственного секторов.

# 1 целевыЕ атакИ

Целевые (таргетированные) атаки — это любое нападение киберпреступников на конкретную выбранную ими цель. Она противопоставляется массовой атаке с помощью вирусов или других вредоносных программ. Для целевых атак характерен взлом и обход защиты жертвы со все более глубоким проникновением в информационную систему. Как правило, массовая атака нацелена против индивидуальных пользователей Интернет, в то время как целевая - против корпоративных сетей.

Среди целевых атак выделяются атаки APT - это продвинутый вариант целевой атаки, когда используются уязвимости 0-day уязвимости, способный пробить любую защиту. Однако данный тип атаки очень дорогостоящий и требует привлечения высококлассных специалистов, в связи с чем наблюдается тенденция к снижению подобного типа атак. Наиболее популярная APT атака, которая у всех на слуху – Stuxnet [2].

Что же касается целевых атак, то они могут быть простыми в техническом плане, однако проводятся успешно, поскольку учитывают все особенностей атакуемой жертвы. Изучаться могут внутренняя структура сети, подключенные АСУ ТП, системы клиент-банк, торговые приложения, инженерные разработки и многое другое. Традиционно целевая атака проводится в несколько этапов: исследование, во время которого проводится анализ векторов проникновения в информационную систему; эксплуатация уязвимости с установкой на устройства жертвы дистанционно управляемого ПО; закрепление в системе с подавлением средств защиты, блокировкой контрольных систем и уничтожением следов проникновения; установка целевого ПО и его эксплуатация [2]. Цели у целевых атак могут быть самые разнообразные: получение доступа к профильной секретной информации (шпионаж), кража средств, персональной и финансовой информации, вмешательство в работу ключевых систем жертвы, вывод из строя оборудования жертвы или нанесение другого вреда (диверсии и саботаж):

* Атака, нацеленная на кражу средств. Подобные атаки проводятся на банки, крупные компании с целью кражи денег со счетов;
* Финансовая информация. В любой компании есть финансовая система, позволяющая вести бизнес. Как правило, это система клиент-банк, но для ретейла это еще и торговые системы. Получив доступ к этой информации или контроль над приложениями, злоумышленники могут ограбить саму компанию или ее клиентов;
* Производственные секреты. Для воровства производственных секретов обычно необходимо атаковать системы разработки инженерных проектов, то есть приложения класса САПР. Такие атаки обычно выполняются под заказ конкурентов или государственных разведок с целью промышленного шпионажа.
* Саботаж. Цель таких атак не в получении данных, а в нарушении работоспособности технологических процессов. Бизнес-модель таких нападений просчитать сложно, поскольку она не выражается в деньгах;
* Персональные данные. Если модули контроля были установлены злоумышленниками в офисных системах, то целью, скорее всего, являются персональные данные клиентов, сотрудников или партнеров. В частности, утечки сообщений электронной почты можно отнести к этому типу атак, хотя чаще переписка утекает с публичных почтовых серверов.

Таким образом, часто основной мишенью для целевой атаки является не компьютерные системы, а сам бизнес целиком.

Есть примеры целевых атак, когда злоумышленники использовали системы предприятия в своих целях. Например, колумбийский картель сломал АСУ морского порта и нужные контейнеры с наркотиками ставили в определенной место автоматически, где его забирали заказчики.

Основным источником угрозы является сложность современных информационных технологий, которые являются очень открытыми и позволяют использовать технологии самым неожиданным образом. Например, встроив вредоносное приложение в JavaScript, в сложном PDF-файле с шифрованным содержимого, который отправляется по почте, вредоносная программа может быть замаскирована также под doc и xls файлы.  Не всегда средства защиты, которые работают на шлюзе, могут распознать вредоносный код, нацеленный против приложения на рабочем месте сотрудника. При этом вариантов различных вложений, присоединений, параллельных загрузок оказывается так много, что отдельные устройства защиты уже не могут достоверно определить вредоносность передаваемой через них информации.

Основная масса  целевых атак проводится через интернет. Для этого злоумышленники могут заразить сайт, который часто посещают потенциальные жертвы, после чего происходит заражение компьютерных систем и проникновение. Также возможно проведение атаки через социальные сети или мессенджеры, когда от человека из списка контактов приходит ссылка с “интересным содержимым”. Вполне понятно, к чему приведет переход по такой ссылке.

Некоторое время назад целевые атаки стали достаточно популярной темой, подогревающей интерес к информационной безопасности. В результате, производители средств защиты выработали несколько инструментов для детектирования целенаправленных атак. Можно указать следующие элементы защиты [2]:

* Песочница. Это виртуальная среда, имитирующая рабочее место сотрудника со всеми установленными программами и компонентами. В ней запускается соответствующее приложение для обработки сообщений и контролируется его поведение. Если приложение ведет себя как-то неадекватно, то сообщение можно заблокировать или передать на подробное изучение в лабораторию производителя. Песочница работает слишком медленно, поэтому вердикт от нее можно получить уже после загрузки файла.
* Репутация. Для веб более действенной может оказаться механизм репутации, когда файл уже раньше был проверен, в том числе и в песочнице, для него сформирован отпечаток, по которому и устанавливается репутация файла. Когда браузер запрашивает файл, то шлюз может проверить его репутацию и в случае подозрений - заблокировать. Если же файла в базе нет, то первый файл пропускается, но передается на анализ в песочницу, чтобы в следующий раз уже более точно знать его репутацию. Работает только для атак типа "охота на китов", которые, собственно, и организуются через веб. Репутация может быть определена не только для файлов, но и для сайтов, и для сообщений электронной почты;
* HIPS (Host-based Intrusion Prevention System, система предотвращения вторжений) или контроль поведения программ. На конечных станциях могут быть установлены специальные агенты, которые контролируют поведение программ. Если программа начинает вести себя как-то подозрительно, то её действия могут быть заблокированы. Например, так можно защититься от шифровальщика, который начинает уничтожать слишком много файлов. Защита этого типа не предотвращает заражение вредоносной программой, но пытается заблокировать само вредоносное действие;
* SIEM (Security information and event management) или управление событиями безопасности. Сразу нужно отметить, что этот механизм не предотвращает атаки, но может обнаружить факт её совершения, выявить путь угрозы и тем самым обнаружить уязвимые точки системы. Этот инструмент собирает информацию из различных источников - песочницы, репутационного сервера, HIPS на местах, межсетевых экранов, антивирусов и множества других средств защиты с целью обнаружить во всех этих данных признаки целенаправленного нападения. Системы этого типа очень сложны в настройке и дают множество ложных срабатываний, но в случае реальной атаки могут сильно помочь в расследовании инцидентов и выявлении уязвимых мест информационной систем для их последующего устранения;
* UEBA [(User and Entity Behavior Analytics)](https://www.anti-malware.ru/analytics/Technology_Analysis/why_technology_UEBA_not_be_silver_bullet) — поведенческий анализ действий пользователя, благодаря данной технологии отмечаются аномалии поведения, указывая на потенциальные угрозы безопасности. Эффективное средство для обнаружения целевых атак и злонамеренной активности.

Следует отметить, что это далеко не полный список инструментов, которые помогают обнаружить целевые атаки, поскольку традиционные средства защиты, такие как антивирусы и межсетевые экраны, также могут оказаться в этом не бесполезны. Теоретически противостоять целевым атакам должна комплексная система безопасности, которая, получив информацию от различных средств защиты и проанализировав ее, могла бы выявить признаки целенаправленной атаки против конкретной системы. Попытки создания подобных комплексных продуктов защиты ведутся, однако проблемой является конкуренция между производителями. Покупать все средства защиты от одного производителя не всегда возможно, а комплексных систем, эффективно работающих со всеми производителями пока разработать не удалось, поскольку не выработаны еще общие стандарты представления информации об инцидентах и протоколы управления. В результате, распределенную по времени атаку выявить и обезвредить оказывается достаточно сложно.

## Диверсии и саботаж выходят на передний план

За последние годы в мире кибершпионажа произошел заметный сдвиг к более открытой деятельности, предназначенной для дестабилизации и дезорганизации целевых организаций и стран. Кибер-атаки против Демократической партии США и последующая утечка похищенной информации была одной из главных тем для обсуждения Президентских выборов в США. Представители разведслужб США приписывают эту кибер-атаку России и характеризуют эту кампанию как успешную, так что, скорее всего, эта тактика будет повторно использована в попытках повлиять на политику и посеять раздоры в других странах.

Кибер - атаки с участием саботажа ранее были традиционно были довольно редки, но в 2016 году были зафиксированы две отдельные волны атак с использованием разрушительного вредоносного программного обеспечения. Вредоносная программа, удаляющая данные на дисках, была использована по целям в Украине в январе и снова в декабре, что привело к отключениям электроэнергии. Одновременно с этим тем троянец Shamoon, удаляющий данные на дисках, вновь появился после четырехлетнего отсутствия и был использован против нескольких организаций в Саудовской Аравии.

Всплеск разрушительных атак совпал со снижением уровня некоторых тайных операций, в особенности в сфере экономического шпионажа, кражи интеллектуальной собственности и коммерческой тайны. Следуя соглашению 2015 года между США и Китаем, в котором обе страны обязались не вести экономический шпионаж в киберпространстве, обнаружение вредоносных программ, связанных с подозреваемыми в шпионаже китайскими группами, значительно сократились. Однако это не значит, что экономический шпионаж полностью исчез, в это же время происходит увеличение других форм целенаправленных атак, таких как подрывная деятельность или высококвалифицированные финансовые атаки.

В 2016 году произошел всплеск саботажных атак, начавшегося с ряда нападений на Украину с использованием вредоносных программ, удаляющих данные на дисках. Эти атаки, возможно, были связаны с другой российской группой кибершпионажа, известной как «SandWorm» (Песчаный червь), и задействовали весьма разрушительного трояна (Trojan.Disakil). Атаки в конце 2015 и начале 2016 года затронули средства массовой информации и энергетический сектор в Украине, причем последнее связано с отключением электроэнергии в стране.

Disakil вернулся в конце 2016 года, когда распространялась его новая версия под видом программы-вымогателя. Вредоносная программа была использована в ряде атак на финансовый сектор в Украине.

Этот вариант вредоносного ПО был разработан для работы на компьютерах Linux и, при запуске, делал их неработоспособными для использования путем шифрования ключевых системных файлов. Как только шифрование заканчивалось, появлялось сообщение с требованием выкупа в 222 Биткоина (приблизительно $210,000 долларов на момент атаки). Выплата выкупа не расшифровывала затронутые файлы с помощью ключей шифрования, генерируемых на зараженном компьютере, и они не сохранялись ни локально, ни на сервере командования и управления (C&C: command and control server). Вредоносная программа была, вероятно, замаскирована под программу-вымогатель для того, чтобы заставить жертв не слишком тщательно расследовать нападение.

Диверсионные атаки также произошли в других регионах, одной из наиболее заметных из которых было возрождение после пятилетнего отсутствия вредоносной программы «Shamoon» (W32.Disttrack), удаляющей данные с дисков. Будучи впервые использован в атаках на энергетический сектор Саудовской Аравии в 2012 году, новый вариант (W32.Disttrack.B) был использован по целям в Саудовской Аравии в ноябре 2016 года и январь 2017.

Первая волна новых атак вредоносной программы была настроена для запуска очистки данных с диска в 20:45 по местному времени в четверг, 17 ноября. Рабочая неделя в Саудовской Аравии длится с воскресенья по четверг. Таким образом, атака была запланирована к запуску после того, как большинство сотрудников возвращались домой на выходные, в надежде снижения вероятности обнаружения до того, как может быть нанесен максимальный ущерб.

Вредоносная программа Shamoon была сконфигурирована с использованием паролей, которые, предварительно были украдены у атакуемых организаций. Скорее всего, эти пароли были использованы, чтобы позволить вредоносному ПО свободно распространяться по сети организации.

Эти нападения, по всей видимости, имели политическую подоплеку. Атаки 2012 года заражали компьютеры, стирая их главные загрузочные записи (MBR) и заменяя их изображением горящего флага США. В последних атаках вместо флага было использовано фото тела Алана Курди, трехлетнего сирийского беженца, утонувшего в Средиземном море в 2015 году.

Ноябрьские атаки были связаны с группой, известной как "Greenbug" (дословно: зеленый баг, ошибка), обнаруженной во время расследования атаки Shamoon. Greenbug была нацелена на ряд организаций на Ближнем Востоке, включая авиационные и энергетические компании, правительство, сферу инвестиции и образования. Greenbug заражала, как минимум, один компьютер системного администратора в организации, которая впоследствии была поражена Shamoon. Январские нападения были совершены группой, известной как "Timberworm" – «Лесной Червь». Хотя Greenbug и Timberworm и кажутся отдельными группами, если они обе распространяют Shamoon, то, скорее всего, это разветвления одной организации.

## Финансовые кражи: злоумышленники теперь нацелены на большие суммы

До недавнего времени киберпреступники в основном ориентировались на клиентов банка, опустошая их счета или похищая данные их кредитных карт. Однако новое поколение злоумышленников имеет большие амбиции и нацеливается на сами банки, иногда пытаясь украсть миллионы долларов за одну атаку. Кибербанды, такие как Carbanak, показали способ, демонстрирующий потенциал этого подхода, провернув ряд атак против банков США.

В течение 2016 года две другие группы подняли ставку, проведя еще более амбициозные атаки. Группе Banswift удалось украсть 81 млн. долларов США из центрального банка Бангладеш, используя недостатки в безопасности банка для проникновения в его сеть, и похитила его учетные данные SWIFT, позволяющие их использовать в мошеннических операциях.

Другая группа, известная как Odinaff, также была уличена в использовании изощренных нападениях на банки и другие финансовые учреждения. Они тоже, как предполагается, использовали вредоносные программы, чтобы скрыть собственные клиентские записи о сообщениях SWIFT, относящихся к мошенническим операциям, осуществляемым группой.

В то время как Banswift и Odinaff демонстрировали технологическое мастерство и применяли передовые тактики, значительно менее опытные группы также украли огромные суммы денег. Мошенничества с компрометацией электронной бизнесс-почты (Business email compromise, BEC), которые полагаются на чуть большее, чем тщательно составленные фишинг-письма, по-прежнему вызывают большие потери: более 3 миллиардов долларов украдено с использованием этой тактики за последние три года.

## Экономический шпионаж

В сентябре 2015 года США и Китай достигли соглашения, что ни одна страна не будет вести экономический шпионаж в киберпространстве. В соответствии с условиями соглашения, обе страны согласились с тем, ни одно правительство не будет «проводить или сознательно поддерживать кражу интеллектуальной собственности, включая коммерческую тайну или другую конфиденциальную деловую информацию, с целью предоставления конкурентных преимуществ компаниям или коммерческим секторам».

Учитывая природу таких шпионских операций, сложно установить, будет ли это соглашение работать. Однако, есть убедительные доказательства того, что было заметное снижение активности в группах, связанных с Китаем, после подписания данного соглашения. Обзор обнаруженных семейств вредоносного ПО, используемых кибер шпионскими группами, которые, предположительно, расположены в Китае, позволил получить понимание степени активности с течением времени. Почти сразу после подписания соглашения количество заражений значительно снизились. Показатели инфицирования продолжали снижаться в следующие месяцы и оставались низкими до конца года.

В сочетании с этой тенденцией некоторые отдельные китайские группы также изменили модель своей деятельности. Например, группа «Buckeye» (aka APT3 или Gothic Panda) занималась кибер-шпионажем против организаций в США, Великобритании и других стран по крайней мере в течение половины десятилетия. Однако, цели группы начали меняться в преддверии Американо-Китайского соглашения.

С июня 2015 года группа начала компрометировать политические лица в Гонконге. К марту 2016 года Buckeye почти полностью перенесла свое внимание на организации в Гонконге. И хотя нет определённых доказательств того, что смена фокуса была обусловлена соглашением, это согласуется с общей тенденцией снижения активности кибер-шпионажа против целей в других странах. Хотя американо-китайское соглашение вызвало смену фокусировки для некоторых групп кибер-атак, это не обязательно означает массовое прекращение операций, связанных со шпионажем.

## Подрывная деятельность как новый объект целенаправленных атак

2016 год был исключительно активным годом для групп, использующих целевые атаки, с заметными инцидентами, произошедшими в Европе, США, Азии и Ближнем Востоке. В течение года уровень высокопрофессиональной активности растет, усиливая политически подрывные действия, направленные против Соединенных Штатов, и разрушительное вредоносное ПО для Саудовской Аравии и Украины. На сегодняшний день действует широкий спектр целевых группировок. В то время, как все мировые державы давно имеют возможность проводить различные кибер-операции, региональные державы также перешли в киберпространство со своими собственными операциями кибершпионажа, направленными против конкурирующих стран и групп внутренней оппозиции. График известных целевых атак отображает 10 из наиболее значимых групп, которые были активны в 2016 году и которые официально связаны с национальным государством.

Ландшафт целевых атак значительно изменился в течение 2016 года, когда несколько групп злоумышленников вышли из тени и участвовали в публичной, политической, подрывной деятельности. Продолжающийся конфликт в Украине, выборы в США и Олимпийские игры, все это пострадало от кампаний, проводимых для кражи и утечки данных, чтобы влиять на общественное мнение, создавать атмосферу недоверия и, возможно, влиять на политические результаты. Благодаря этим успехам, в выборах 2017 года в ряде стран также были использованы кибер-атаки, связанные с подрывной деятельностью. Группы злоумышленников между тем постоянно совершенствуют свою тактику, несколько удаляясь от использования персонализированного вредоносного ПО и все больше полагаясь на законные программные инструменты для компрометации целевых сетей.

Одним из наиболее бросающихся в глаза событий в 2016 году стала значимость операций, пытающихся влиять на политические события в целевых странах. Традиционно группировки целевых атак сосредоточились на шпионаже и старались не привлекать внимание к своей деятельности во избежание обнаружения, но несколько группировок добавили больше открытых операции в свой арсенал средств в 2016 году.

В августе 2016 года драгоценные данные, связанных с кибершпионской группировкой «Equation Group», были выложены в сеть группой, называющей себя "Теневые Брокеры". Утечка содержала инструменты и эксплойты, используемые «Equation Group», и "Теневые Брокеры" утверждали, что это была часть от того, что они заполучили, предлагая на торгах остальное тому, кто больше заплатит. Большинство слитых файлов было несколько летней давности, датируясь между 2010 и 2013 годами. Как они попали в руки о лидерах остается неизвестным. Группа "Теневые Брокеры" была неизвестна до этого инцидента, но это также может быть прикрытием для другой группировки.

Учитывая то, что попытки "Теневых Брокеров" продать украденные данные были весьма вялыми, вполне возможно, что дискредитация «Equation Group», а не денежная прибыль, была основным мотивом, стоящим за утечкой этих данных.

Самым громким, диверсионным инцидентом в этом году был ряд вторжений против Демократической партии, которые произошли в преддверии президентских выборов в 2016 году в США. Совместное расследование со стороны разведывательного сообщества США пришло к выводу, что две группы, связанные со службой разведки России, были ответственны за эту кампанию.

Обе группы были известны и ранее тем, что в течение ряда лет активно занимались шпионажем против ряда целей в США и Европе. Группа Fritillary (Рябчик, также известна как APT29 и Cozy Bear) была активна, по крайней мере, с 2010 года и был известна использованием троянов семейства «Duke» против своих целей, например, Cozyduke (Trojan.Cozer) и Seaduke (Trojan.Seaduke). Группа Swallowtail (Махаон, также известна как APT28 и Fancy Bear) была активна как минимум 10 лет и обычно использует Sofacy Trojan (Infostealer.Sofacy) в качестве одного из основных вредоносных инструментов. Рябчик известен нацеленностью на очень высокопоставленных лиц и организации в правительстве, международную политику и научно-исследовательские институты Европейского Союза и Соединенных Штатов, тогда как группа Махаон главным образом нацелена на войска, правительство, посольство, и штат военных подрядчиков в странах Восточной Европы.

В сентябре группа Махаон также была причастна к утечке медицинских записей, похищенных у Всемирного антидопингового агентства (ВАДА). Данные, касающиеся американских олимпийских спортсменов, британских велосипедистов и спортсменов из ряда других стран, были опубликованы после несанкционированного проникновения.

По данным ВАДА, ответственным за вторжение был Махаон. Группа сделала необычный шаг, создав свой собственный вебсайт (используя прозвище «Fancy Bear») для того, чтобы опубликовать украденные данные вместе с утверждением о наличии доказательств нарушения спортсменами антидопинговых правил.

Несанкционированное проникновение в DNC (Демократический национальный комитет) и WADA было основным изменением в тактике обеих групп, обе ранее не занимались этим видом подрывной деятельности. Отчет Разведывательного сообщества США о кражах данных DNC и последующее публичное раскрытие информации расценивается как часть кампании влияния, проводимая российским Правительством, направленной на президентские выборы в США в 2016 году. Был также сделан вывод о том, что в России эта кампания была сочтена успешной и что эти мероприятия, вероятно, будут служить источником информации для проведения будущих операций влияния.

Учитывая доказанный потенциал нагнетания разногласий и путаницы, существует большая вероятность того, что эта тактика может быть использована снова в попытке дестабилизировать другие страны. Франция и Германия проводили выборы в 2017 году, и Бруно Каль, глава Службы внешней разведки ФРГ, заявил, что атаки того же типа уже проводились против Германии. “У нас есть доказательства кибератак, которые не имеют никакой другой цели кроме как вызвать политическую неопределенность", - сказал он. “Преступники заинтересованы в делегитимизации демократического процесса как такового, неважно кому это впоследствии поможет”.

# 2 Тактики целевых атак



## Уязвимости нулевого дня

Уязвимости «нулевого дня», — уязвимости, не обнаруживаемые поставщиками противовирусного программного обеспечения. По этому показателю «нулевые дни», определенные в течение 2016 года, в очередной раз упали, незначительно снизившись с 4066 до 3986 [1]. Этот падение говорит о растущей популярности программ поощрения "bug bounty” и большем фокусе на безопасность как части процесса разработки программных продуктов. Это может означать, что для атакующих находить уязвимости нулевого дня становится все труднее, заставляя их отойти от использования уязвимостей «нулевого дня» и расширить спектр используемых тактик, например, «Living off the Land».

Снижение обнаружений уязвимостей нулевого дня происходит после того, как подпольный рынок уязвимостей оказался в центре внимания в 2015 году, после взлома компании «Hacking Team» (компания, специализирующаяся на разработке шпионского программного обеспечения для спецслужб со всего мира). Множественные эксплойты уязвимостей нулевого дня утекли в результате этого взлома, в дополнение к информации о том, за какие деньги эти эксплойты обменивались.

Тем не менее, было множество случаев использования уязвимостей нулевого дня при целевых атаках во время 2016. Например, в октябре Adobe выпустила патч для ПО «Flash Plasyer» после выявления уязвимости нулевого дня, которая активно эксплуатировалась «In the Wild» (термин, означающий свободное распространение на компьютерах пользователей). Три уязвимости в Apple iOS, в совокупности известные как Trident, были раскрыты и исправлены в августе после того, как они были обнаружены в кибератаке против правозащитника из ОАЭ. В мае Microsoft исправил уязвимость нулевого дня в Internet Explorer, который использовался в целевых атаках в Южной Корее.

Аналогичным образом число уязвимостей в промышленных системах управления (ICS), обнаруженных в течение 2016 года, упало по сравнению с 2015 годом, дополнительно подтверждая предположения о том, что для атакующих становится все труднее найти уязвимости.

## Living off the land

Злоумышленники, от киберпреступников до спонсируемых государством групп, начали менять свою тактику, все больше используя особенности операционной системы, уже имеющихся в наличии инструменты и облачные службы для компрометации своих жертв. Самый громкий случай атаки “Living off the land” произошел во время выборов в США. Простое «spear-phishing» (эта атака использует технологии фишинга, но нацелена на одну «жертву») электронное сообщение предоставило доступ к учетной записи Gmail председателя кампании Хиллари Клинтон Джона Подеста без использования каких-либо вредоносных программ или уязвимостей.

Нападающие начали менять свою тактику, расширяя ряд инструментов, и многие группировки больше не так уверены в традиционных инструментариях атак вроде вредоносных программ и уязвимостей нулевого дня. Хотя это не новый способ, группы все чаще «живут за счет земли», используя особенности операционной системы, законные программные средства, и облачные сервисы для компрометации сетей. Эта тактика может сделать атаки более трудными для обнаружения, так как выявление злонамеренного использования законных инструментов сложнее по сравнению с выявлением присутствия вредоносных программ.

Атака «Living off the land» предполагает использование имеющихся ресурсов, а не вредоносного программного обеспечения и эксплойтов, и предоставляет много преимуществ для злоумышленников. Выявление и использование уязвимостей нулевого дня стало сложнее, так как произошли улучшения в развитии информационной безопасности и в программе поощрений "bug bounty”. Инструментарий для веб-атак уже не пользуется такой популярностью, вероятно, из-за усилий, необходимых для разработки новых эксплойтов и базовой инфраструктуры.

Мощные средства сценариев, такие как PowerShell и макросы — стандартные компоненты Windows и Microsoft Office, которые могут упростить удаленный доступ и загрузку вредоносного программного обеспечения без использования уязвимостей или вредоносных инструментов. Несмотря на двадцатилетнее существование, офисные макросы вновь возродились в сфере угроз, поскольку злоумышленники используют методы социальной инженерии для облегчения преодоления мер безопасности, которые были введены в действие ранее для решения прежних проблем с макровирусами. Когда все выполнено хорошо, метод «Living off the land» может привести к почти бессимптомному инфицированию, позволяя злоумышленникам «прятаться, оставаясь на виду».

### Как группа Timberworm использовала тактику "жить за счет земли"

Одним из известнейших представителей «жизни за счет земли» в 2016 году были Timberworm, группа кибершпионажа, связанная с возобновлением атак с участием вредоносного разрушительного ПО Shamoon (W32.Disttrack.B). Шамун появился в ноябре 2016 года после четырехлетнего отсутствия с серией атак на цели в Саудовской Аравии. Еще две волны атаки произошли позже в Ноябре 2016 года и январе 2017.

В то время как ноябрьские атаки были связаны с группой, известной как “Greenbug”, атаки в январе были запущены «Timberworm», группа кибершпионажа, ответственная за ряд атак по всему Ближнему Востоку.

Чтобы распространить Shamoon, Timberworm сначала отправила spear-phishing электронное сообщение отдельным лицам в целевых организациях. В некоторых случаях, сообщения содержали файлы Microsoft Word или Excel в виде вложений. В других письмах содержались вредоносные ссылки, по которым, в случае нажатия, скачивались аналогичные файлы Word или Excel.

Если файл был открыт, макрос запустил сценарий PowerShell, который предоставлял удаленный доступ и выполнял базовое сканирование скомпрометированного компьютера. Если компьютер представлял интерес, то затем на него устанавливалась вредоносная программа (Backdoor.Mhretriev).

Через него нападавшие использовали имеющиеся в изобилии легальные средства для администрирования и тестирования на проникновение, чтобы просмотреть сеть и идентифицировать другие компьютеры для заражения. К ним относятся:

* PsExec - инструмент для выполнения процессов в других системах от Microsoft Sysinternals;
* PAExec - бесплатная реализация PsExec из Poweradmin;
* Сетевой сканер Netscan, многоцелевой сетевой сканер IPv4 / IPv6;
* Samdump, инструмент взлома, который сбрасывает хэши пароля Windows ;
* Mimikatz (Hacktool.Mimikatz), инструмент взлома, используемый для сбора учетных данных;
* TightVNC, приложение для доступа к удаленному рабочему столу с открытым исходным кодом;
* Plink, средство для сетевого подключения из командной строки, поддерживающее зашифрованное соединение;
* Rar, утилита архивирования для сжатия файлов перед эксфильтрацией.

После завершения разведывательной операции Shamoon устанавливался на предварительно отобранные компьютеры. Вредоносная программа была настроена для запуска очистки информации с диска в установленное время на всех взломанных компьютерах, увеличивая эффект воздействия от нападения.

### Инструменты, используемые злоумышленниками

Согласно телеметрии репутации файлов Symantec [1], наиболее часто используемыми легальными инструментами, которыми могли злоупотреблять атакующие в 2016 году, были Mimikatz, PsExec, и WCE.

Наиболее широко известным легальным инструментом, который мог быть неправомерно использован злоумышленниками в течение 2016 года, был Mimikatz (Hacktool.Mimikatz) - инструмент, способный вносить изменения в привилегии, экспортировать сертификаты безопасности и восстанавливать пароли Windows в открытом тексте. За ним следуют утилита PsExec от Microsoft Sysinternals и редактор учетных записей Windows (Windows Credential Editor). Учитывая огромное количество таких случаев и тот факт, что все три инструмента могут иметь легальное применение (даже Mimikatz можно использовать для тестирования на проникновение), легко увидеть привлекательность этих инструментов для злоумышленников, поскольку их использование может пройти незамеченным.

Вредоносные скрипты PowerShell также широко используются в целенаправленных атаках, злоумышленники используют гибкость этой структуры для нужных загрузок, просмотра скомпрометированных сетей, и проведения разведки. Недавние исследования Symantec [1] продемонстрировали популярность PowerShell в качестве инструмента атаки. Из всех сценариев PowerShell, проанализированных с помощью песочницы Symantec’s Blue Coat Malware Analysis для анализа вредоносных программ, 95.4% были вредоносными [1].

Другой пример атаки «living off the land» осуществлялся кибершпионажной группировкой «Chafer» (дословно – майский жук), которая, как предполагается, базируется в Иране. Одним из векторов его атаки является взлом веб-серверов, используя уязвимости, выявленные с помощью средств веб-сканирования. В недавнем вторжении против целей в Турции было обнаружено, что Chafer использовала программный инструмент JexBoss для идентификации старой, непатченной, общественной (бесплатной) версии сервера приложений JBoss, принадлежащей целевому объекту. Затем группа развернула на сервере веб-оболочку, скрипт, который разрешил удаленное администрирование, в дополнение к копии программного обеспечения Mimikatz.

С его помощью они смогли использовать собственные средства операционной системы, такие как Qwinsta и Whoami, для извлечения информации о скомпрометированном сервере. В течение 20 минут после компрометации, группа использовала инструмент PsExec от Microsoft Sysinternals для распространения на два других компьютера в атакуемой сети.

Еще одним субъектом, который использовал эту тактику в последнее время, является китайская группа «Tick» (Клещ), которая нацелилась главным образом на японские организации старше 10 лет. В недавно проведенных кампаниях было видно, что они использовали spear-phishing электронные сообщения и взлом японских веб-сайтов для их заражения.

Одним из основных инструментов группы Tick является вредоносное ПО собственной разработки (Backdoor.Daserf), но она также использует и ряд вышеупомянутых инструментов, таких как Mimikatz, редактор учетных записей Windows, и Gsecdump. Gsecdump - хакерский инструмент, который может быть использован для кражи хэшей из менеджера безопасности учетных записей (SAM), Активного Каталога (Active Directory), и активных сеансов входа в систему.

Есть также случаи, когда злоумышленники используют базовые облачные сервисы, а не серверы управления и контроля, для эксфильтрации данных. Например, было установлено, что «Fritillary», одна из групп, атаковавших DNC, использовала приблизительно 200 учетные записей Microsoft OneDrive для того, чтобы скачать украденные данные. Предположительно цель этого была в том, чтобы скрываться, оставаясь на виду, нападавшие рассчитывали, что данные, перемещаемые в OneDrive, могут быть ошибочно приняты жертвой за обычную активность.

## Электронная почта как предпочтительный канал для атаки

На сегодняшний день, наверное, самый массовый способ вторжения на компьютеры пользователей Интернета – рассылка вредоносных программ (вирусов) по электронной почте. Вирус присоединяется к письму, и жертву провоцируют на то, чтобы этот вирус запустить. Для этого вирус необходимо замаскировать: под полезную программу, картинку, безобидный документ или что-то еще, а в само письмо включить провокационный текст.

Необходимо понимать, что письма, зараженные вирусом, может рассылать не только автор вируса или другой злоумышленник. Если компьютер стал жертвой вируса, он может самостоятельно распространять вирус, без ведома владельца зараженного компьютера. Поэтому неудивительным является получение вредоносных писем от известного адресанта, в то время как он не имеет к этому письму никакого отношения.

Вредоносные письма стали излюбленным оружием для широкого спектра кибератак в 2016 году и использовались всеми, начиная с групп кибершпионажа при государственной поддержке, и заканчивая массовыми рассылками программ-вымогателей мошенническими группировками. Каждое 131 отправленное сообщение было злонамеренным, и это самый высокий показатель за пять лет [1]. Возрождение популярности электронной почты было обусловлено несколькими факторами. Это проверенный годами канал атаки. Он не полагается на уязвимости, а использует вместо этого простые уловки, чтобы соблазнить жертв открыть вложения, проследовать по ссылке или раскрыть свои учетные данные. Сообщения «Spear-fishing», например, поддельные электронные письма, инструктирующие жертвы как сбросить пароль Gmail, были использованы в США при атаках на выборах.

Вредоносные письма, замаскированные под обычную переписку, такие как счета-фактуры или уведомления о доставке, одновременно с этим выступали как предпочтительное средство распространения вымогателей. Распространенность спам-ботнетов «botnets-for-hire», таких, как Necurs, позволило группам вымогателей проводить массовые кампании по рассылке электронных сообщений в течение 2016 года, доставляя сотни тысяч вредоносных писем ежедневно.

### Вредоносные программы

Хотя электронная почта и является жизненно важным инструментом коммуникации, она также является одним из главных источников нарушений для конечных пользователей и организаций. Это нарушение может варьироваться от нежелательных писем в виде спама до более опасных угроз, таких как распространение программ-вымогателей или целенаправленных фишинг-рассылок.

Хотя спам составляет чуть более половины всех электронных писем (53%), растущая доля этого спама содержит вредоносные программы. Это увеличение количества распространяемых по электронной почте вредоносных программ произошло в основном благодаря профессионализации вредоносных почтовых операции. Создатели вредоносных программ для их рассылки могут воспользоваться аутсорсингом специализированных групп, которые проводят крупные спам-кампании. Сами масштабы почтовых операций с вредоносными программами указывают на то, что злоумышленники получают значительную прибыль от таких атак и электронная почта останется одним из основных направлений атак в 2017 году.

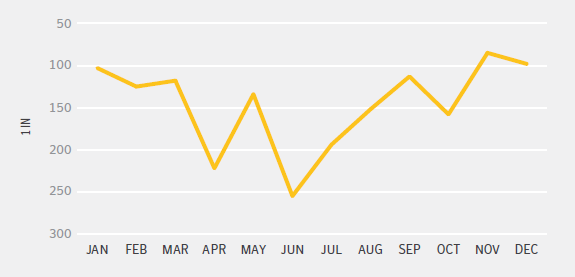
Собранные за 2016 год данные электронной почты наглядно показывают, что электронная почта стала основным вектором распространения вредоносного ПО [1].

Наиболее примечательной тенденцией, наблюдавшейся за 2016 год, было повышение доли распространения вредоносных программ в электронных почтовых сообщениях. Их соотношение увеличилось с «1 из 220» в 2015 году до «1 из 131» в 2016 году.

Это увеличение в 2016 году доли вредоносного ПО электронной почте может быть связано с непрекращающейся массовой рассылкой вредоносных программ, в основном, «Locky», «Dridex» и «TeslaCrypt». Одним из основных распространителей вредоносного ПО является ботнет, известный как Necurs (Backdoor.Necurs). Necurs несет ответственность за массовые рассылки, распространяющие вредоносное ПО через JavaScript и макросы офисных документов. Эти загрузчики впоследствии устанавливали полнофункциональное содержимое, которым в 2016 году, как правило, были программы-вымогатели, такие, как Locky.

Necurs бездействовал с 24 декабря 2016 года по 20 марта 2017, и это означало, что произошел значительный спад в доле вредоносных программ в электронных сообщениях в январе и феврале 2017 года. Хотя перерыв на время Рождества не является необычным для групп, занимающихся вредоносными программами, эти перерывы обычно продолжаются только неделю. Причины для прекращения деятельности Necurs остаются неизвестными, но группа смогла немедленно возобновить кампании массовой рассылки по его возвращению. Системами фильтрации было заблокировано почти два миллиона вредоносных электронных сообщений только 20 марта, в день его возвращения.

Dridex - это финансовый троян, используемый для кражи банковских учетных данных у конечных пользователей. Злоумышленники, стоящие за Dridex, - профессионалы, которые приложили много усилий на постоянное совершенствование вредоносного ПО, делая электронные письма, используемые для его распространения, похожими на настоящие, насколько это возможно. TeslaCrypt и Locky - это программы-вымогатели, Locky появился в феврале 2016 года. Программы-вымогатели были одной из основных тем кибербезопасности в 2016 году. Ежемесячная телеметрия, собираемая Symantec [1], показала высокий начальный импульс в году для вредоносного ПО из электронной почты, с резкими падениями в апреле и в июне, в то время, когда уменьшалась активность групп, стоящих за Locky, Dridex и другими (Рисунок 1).



*Рисунок 1 — ежемесячная доля вредоносного программного обеспечения в почтовых сообщениях*

Cчитается, что снижение активности в апреле и июне обусловлено деятельностью правоохранительных органов, после ареста 50 человек в России, предположительно связанных с банковской мошеннической группировкой «Lurk». Однако это снижение активности было лишь временным и рассылки со спамом нежелательной почты быстро увеличились. Кампании с участием Dridex и Locky возобновились, хотя число случаев угроз семейства Kovter (Trojan.Kovter) в августе начало увеличиваться и продолжало расти в течение оставшегося года.

В 2016 году оптовая торговля и сельское хозяйство были классифицированы как отрасли промышленности наиболее пострадавшие от угроз, связанных с электронной почтой (Рисунок 2)

|  |  |
| --- | --- |
| **Отрасль промышленности** | **Доля вредоносных почтовых сообщений (1 из)** |
| Не классифицируемые учреждения | 103 |
| Сельское и лесное хозяйство, рыболовство | 111 |
| Оптовая торговля | 111 |
| Услуги | 121 |
| Производство | 130 |
| Розничная торговля | 135 |
| Добыча полезных ископаемых | 139 |
| Государственное управление | 141 |
| Транспорт и коммунальные службы | 176 |
| Строительство | 179 |
| Финансы, страхование, недвижимость | 182 |

*Рисунок 2 — соотношение распространения вредоносных программ в почтовых сообщениях по отраслям*

За исключением розничной торговли, которая показала падение в уровне вредоносного ПО в электронной почте (от «1 из 74» писем в 2015 году до «1 из 135» писем в 2016), в 2016 году каждой отрасли увеличилось количество вредоносных программ. Наибольшее увеличение произошло в отраслях транспорта (от «1 из 338» писем до «1 из 176»), финансах (от «1 из 310» до «1 из 182»), и добыче полезных ископаемых» (от «1 из 304» до «1 из 139»). Здравоохранение продемонстрировало существенный рост от «1 из 396» сообщений до «1 из 204».

В 2016 году вредоносное ПО в электронной почте затронуло бизнес любых масштабов. Однако, малый и средний бизнес (от 251 до 500 сотрудников) пострадали больше всего (Рисунок 3).

|  |  |
| --- | --- |
| **Размер компании** | **Доля вредоносных почтовых сообщений (1 из)** |
| 1 – 250 | 127 |
| 251 – 500 | 95 |
| 501 – 1000 | 139 |
| 1001 – 1500 | 224 |
| 1501 – 2500 | 104 |
| 2501+ | 170 |

*Рисунок 3 — соотношение распространения вредоносных программ в зависимости от размера компании*

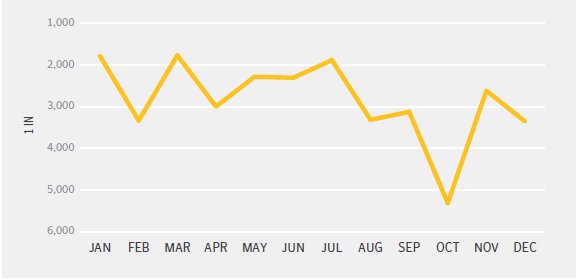
Самый высокий уровень вредоносного ПО в почтовом трафике был в компаниях с численностью 251-500 человек, в них на 95 полученных сообщений одно содержало вредоносное ПО.

### Фишинг

В течение нескольких последних лет доля фишинговых сообщений снижалась, и в 2016 году она снова упала, снизившись с «1 из 1846» в 2015 электронных писем до «1 из 2596» писем в 2016.

В октябре произошло значительное падение, в котором доля фишинга составила только «1 из 5 313» писем, прежде чем она вернулась к более «среднему» значению «1 из 2621» писем в ноябре (Рисунок 4).

В октябре в мире информационной безопасности произошло много событий, в том числе ботнет «Mirai», который стал более заметным после распределенной атаки на отказ в обслуживании (DDoS) на DNS-провайдер Dyn, который затронул ряд известных сайтов, включая Spotify, Netflix и PayPal. Также поступали сообщения об увеличении активности «Kovter» из семейства угроз (Trojan.Kotver). Однако нет ни одного внятного объяснения, почему доля фишинга так резко снизилась в этом месяце.



*Рисунок 4 — «Ежемесячная доля фишинговых сообщений».*

Вероятно, есть множество причин снижения фишинговой активности. Пользователи все больше осознают опасности нажатия неизвестных ссылок или загрузки подозрительных вложений, что означает, что, возможно, «стандартные», неизбирательные, массовые рассылки фишинговых сообщений становятся менее эффективны для мошенников.

Сельское хозяйство было наиболее подвержено фишингу в 2016 году, при этом 1 из 1,815 электронных сообщений классифицировалось как попытка фишинга (Рисунок 5).

|  |  |
| --- | --- |
| **Отрасль промышленности** | **Доля фишинговых сообщений (1 из)** |
| Сельское и лесное хозяйство, рыболовство | 1815 |
| Финансы, страхование, недвижимость | 1918 |
| Добыча полезных ископаемых | 2254 |
| Государственное управление | 2329 |
| Розничная торговля | 2419 |
| Не классифицируемые учреждения | 2498 |
| Услуги | 3091 |
| Производство | 3171 |
| Оптовая торговля | 4742 |
| Строительство | 4917 |
| Транспорт и коммунальные службы | 6176 |

*Рисунок 5 — соотношение фишинговых сообщений по отраслям*

Самый высокий уровень фишинга произошел в компаниях с численностью 251-500, где 1 из 2554 полученных писем классифицировалось как попытка фишинга (Рисунок 6).

|  |  |
| --- | --- |
| **Размер компании** | **Доля фишинговых сообщений (1 из)** |
| 1 – 250 | 2897 |
| 251 – 500 | 2554 |
| 501 – 1000 | 4023 |
| 1001 – 1500 | 6640 |
| 1501 – 2500 | 2610 |
| 2501+ | 3323 |

*Рисунок 6 — соотношение распространения фишинговых сообщений в зависимости от размера компании*

Тем не менее, атаки «spear phishing» продолжают расти. В течение 2016 года было много громких случаев использования атак «spear phishing», таких, как взлом электронной почты председателя избирательной кампании Хиллари Клинтон Джона Подеста и бывшего госсекретаря США Колин Пауэлла.

Эта практика широко используется целым рядом групп в последнее время. Важным примером является вышеупомянутое вторжение в DNC в преддверии выборов президента США. Одной из отправных точек для компрометации, согласно данным ФБР, была отправка сообщения типа spear-phishing на электронную почту председателя кампания Джона Подеста 19 марта 2016 года. Письмо было создано так, как будто оно пришло с официального аккаунта администратора Gmail, в нем сообщалось, что его электронная почта была скомпрометирована, и переправляла его на сброс пароля по сокращенному URL-адресу, который скрывал вредоносный URL. После перехода по ссылке жертва была направлена к фальшивой странице сброса пароля, маскирующейся под настоящую страницу сброса учетной записи Gmail. Никакие вредоносные программы или эксплойты не понадобились для выполнения этой атаки. Вместо этого для получения пароля были использованы простые методы социальной инженерии.

### Программы-вымогатели

Программы-вымогатели продолжают поражать организации и пользователей, без разбора пересылая огромные объемы вредоносных писем. В некоторых случаях организации могут быть перегружены огромным объемом полученных писем, содержащих программы-вымогатели. Злоумышленники требуют все больше и больше от жертв, средняя сумма с требованием выкупа в 2016 году выросла до $1,077, по сравнению с $294 годом ранее.

Злоумышленники довели до совершенства бизнес-модель, обычно предусматривающую использование вредоносных программ, скрытых в безобидных электронных письмах, не взламываемое шифрование, и анонимный выкуп с использованием криптовалют. Успех этой бизнес-модели отметился ростом количества примкнувших к ней злоумышленников. Число новых семейств программ-вымогателей, обнаруженных в течение 2016 года, более чем утроился и достиг 101, а Symantec зарегистрировал [1] 36-процентное увеличение заражение вымогателями.

### Интернет вещей (IoT) и облачные технологии

В то время, как вымогатели и группы финансового мошенничества продолжают представлять самую большую угрозу для конечных пользователей, другие угрозы только начинают появляться. Это был только вопрос времени, прежде чем атаки на устройства из интернета вещей начнут набирать обороты, и в 2016 году произошел первый крупный инцидент с появлением Mirai, ботнета, состоящего из устройств IoT, таких как маршрутизаторы и камеры безопасности. Слабая внутренняя безопасность этих устройств сделала их легкими для захвата злоумышленниками, которые создали достаточно большой ботнет для реализации самой масштабной когда-либо виденной DDoS-атаки. За 2016 год было зарегистрировано двукратное увеличение попыток атак на устройства IoT, а во время пиковой активности, в среднем, одно устройство IoT было атаковано раз в две минуты.

Некоторыми целями Mirai были облачные сервисы, такие как DNS-провайдер Dyn. В сочетании со взломом миллионов баз данных MongoDB, размещенных в облаке, это продемонстрировало, как атаки на облачные сервисы стали реальностью и, вероятно, увеличатся в 2017. Растущая зависимость от облачных сервисов должна стать предметом озабоченности организаций, поскольку они представляют собой слепую зону относительно информационной безопасности. В среднем организация использует 928 облачных приложений, по сравнению с 841 в начале этого года [1]. Однако большинство ИТ-директоров считают, что их организации использует только около 30 или 40 облачных приложений, это означает, что уровень риска может быть недооценен, оставляя их открытыми для атаки от вновь возникающих угроз.

## Появление новых угроз

В дополнение к текущей деятельности известных групп целенаправленных атак, в 2016 году из тени вышли другие угрозы. В августе была обнаружена прежде неизвестная группа, называющаяся «Strider», которая организовывала атаки на отдельные цели в России, Китае, Швеции и Бельгии [1].

Основным инструментом Strider является скрытый троян, известный как Remsec (Backdoor.Remsec), который, имеет такую высокую степень сложности, что, по оценкам экспертов, первоначально он был сконструирован для целей шпионажа. Будучи активным начиная, по крайней мере, с 2011 года, Strider поддержал низкий уровень активности отчасти потому, что он был очень избирательным в выборе целевых показателей, при этом были обнаружены признаки инфицирования 36 компьютеров в семи отдельных организациях.

Remsec продемонстрировал высокую степень технической компетентности, содержащий ряд дополнительных функций, предназначенных для обхождения обнаружения. Несколько компонентов были в форме исполняемых BLOBs (Binary Large Objects, двоичный большой объект), которые сложнее обнаружить традиционному антивирусному программному обеспечению, основанному на сигнатурах. В дополнение к этому большая часть функциональности вредоносного ПО развертывается по сети, то есть он находится только в памяти компьютера и никогда не хранится на диске — это опять делает его обнаружение еще сложнее.

Remsec наглядно демонстрирует уровень навыков и средств, с которым государственные группы теперь могут воздействовать на цели.

# ЗАКЛЮЧЕНИЕ

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. В отличие от угроз прошлого, которые могли отформатировать жесткий диск или порадовать ничего не подозревающего владельца компьютера всякими неожиданными эффектами, сегодня вредоносные программы стараются маскироваться и скрывать свою деятельность, чтобы втайне выполнять заложенные в них функции.

В ходе данной работы были проанализированы кибер - атаки последних лет. В результате можно сделать вывод о том, что в деятельности кибер - преступников наметился ряд тенденций:

* Кибер - атаки в подрывных целях, например, во время выборов в США и во время Олимпийских игр, выходят на первый план и представляют собой новую форму высокопрофессиональной целевой атаки;
* Все чаще используются целевые атаки с использованием разрушительного ПО в корпоративных, государственных и финансовых секторах;
* Экономический шпионаж, например, кража торговых или коммерческих секретов, являющийся одной из традиционных форм целевых атак, в некоторых случаях снизился. Обнаружение китайских вредоносных программ для шпионажа значительно упало после взаимного соглашения с США и Китая не нацеливаться на интеллектуальную собственность. Однако, экономический шпионаж полностью не исчез и его снижение происходит то время, когда уровень других типов целевых атак, таких, как саботаж и диверсии, растет;
* Уязвимости нулевого дня стали менее важными и некоторые злоумышленники больше не полагаются на вредоносные программы, все чаще используя тактику “living off the land” — подручные инструменты, включая легальные средства для администрирования и тестирования на проникновение, для проведения атак;
* Сейчас, когда даже в кофеварки и холодильники встраиваются технологии IoT, а защита в них практически не предусмотрена, начинают активно развиваться угрозы, связанные с эксплуатацией устройств интернета вещей злоумышленниками.

На основании перечисленных выше тенденций можно сделать выводы и об актуальных способах защиты от этих угроз:

* Необходимо придать особое значение множественным, перекрывающимся и поддерживающим друг друга защитным системам для защиты критических точек от отказа в любой конкретной технологии или методе защиты. Это должно включать развертывание регулярно обновляемых брандмауэров, а также шлюзовые антивирусы, системы обнаружения вторжений или защиты (IPS), защиту уязвимостей веб-сайтов от вредоносных программ и обеспечение безопасности сетевых шлюзов по всей сети;
* Эксплуатация уязвимостей – это наиболее широко используемая тактика групп целенаправленных атак. Необходимо получать своевременные оповещения о новых уязвимостях и угрозах на платформах поставщиков и исправлять известные уязвимости как можно скорее;
* Необходимо внедрять и обеспечивать соблюдение политик безопасности, при которых любые конфиденциальные данные шифруются при хранении и в процессе передачи. Пользовательские данные также должны быть зашифрованы. Это может помочь снизить ущерб от потенциальных утечек данных из организации;
* Атакующие часто используют украденные или учетные данные по умолчанию для перемещения по сети. Поэтому стоить уделить внимание парольной политике. Важные пароли, например, с высокими привилегиями, должны иметь длину не менее 8-10 символов (предпочтительно больше) и включать в себя сочетания букв и цифр. Пользователям следует избегать повторного использования одних и тех же паролей на нескольких сайтах и обмениваться паролями с другими пользователями, не забывать менять пароли по-умолчанию, особенно это актуально для устройств интернета вещей;
* Необходимо периодически оповещать и просвещать сотрудников об опасностях, связанных с фишинговыми электронными сообщениями, в том числе о необходимости проявлять осторожность с электронными сообщениями из незнакомых источников и при открытии вложений, которые не запрашивались, даже от известного адресанта.

Защита от целевых атак - это комплексная задача, которую нельзя решить, используя один какой-либо продукт информационной безопасности. Для достижения цели требуется применять весь спектр средств, только в этом случае можно повысить процент успешного обнаружения атак.

# Список использованных источников

1. Internet Security Threat Report [Электронный ресурс]. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
2. Целевые атаки (APT) [Электронный ресурс]. URL: https://www.anti-malware.ru/threats/target-attack
3. Бокарев, Т. Энциклопедия Интернета. М.: Изд-во ПРОМО-РУ, 2012.- 241 с.
4. Сосновский, Р. И. Основы безопасности в Интернете. - СПб.: Питер, 2012 – 512с.
5. SecurityLab. [Электронный ресурс]. URL: http://securityLab.ru