Сергей И. Журин[1,2], Дмитрий Е. Комарков[3]
[1]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[2]АО «Федеральный центр науки и высоких технологий «Специальное научно-производственное объединение «Элерон»,
ул. Генерала Белова, 14, г. Москва, 115563, Россия
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА

DOI: http://dx.doi.org/10.26583/bit.2018.4.09

Аннотация. Целевой фишинг является одним из методов социальной инженерии. При целевом фишинге текст электронного письма составляется с учетом знаний о конкретном предприятии и сотруднике (часто) с использованием знаний социологии и психологии таким образом, чтобы вызвать желание открыть прикрепленный файл или нажать на ссылку. Основная трудность защиты от такого письма состоит в том, что методы автоматизированного анализа не дают гарантии его обнаружения, т.к. современные киберпреступники используют новые текстовые формулировки, уязвимости нулевого дня, а также средства автоматизации для инжектирования эксплойтов в файлы, что снижает эффективность сигнатурного анализа антивирусных программ. Каждая из существующих технологий обнаружения в отдельности не позволяет обеспечить защиту от целевого фишинга. Однако объединение технологий (фильтрация спама, межсетевые экраны, антивирусы) с обязательным включением организационных мер, в том числе обучения и тестирования персонала, позволяет в комплексе защитить внешний информационный периметр организации от целевого фишинга. В статье приведен детальный анализ технологии реализации целевого фишинга с анализом причин возможностей его реализации двумя типовыми методами: запуском эксплойта при переходе по ссылке и при запуске файла. Приведен обзор уязвимостей 2016 – 2017 года, использованных для целевых атак. Приведены современные технологии защиты и их сравнительный анализ. Отмечено, что каждая из технологий не позволяет в отдельности обеспечить защиту от целевого фишинга. Предложены наиболее эффективные современные методы защиты на основе их сравнительного анализа и анализа современных информационных угроз.

Ключевые слова: APT, фишинг, целевой фишинг, социальная инженерия, внедрение ПО.
Для цитирования: ЖУРИН, Сергей И.; КОМАРКОВ, Дмитрий Е. ЗАЩИТА ВНЕШНЕГО ИНФОРМАЦИОННОГО ПЕРИМЕТРА ОРГАНИЗАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 95-107, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1164>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.09.

Sergey I. Zhurin[1,2], Dmitry E. Komarkov[3]
[1]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
[2]Joint Stock Company "Federal Center of Science and High Technologies "SNPO "Eleron",
14, Gen. Belova str., Moscow, 115563, Russia
e-mail: sizh@mail.ru, http://orcid.org/0000-0002-1538-0267
[3]National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
e-mail: dimank989898@gmail.com, http://orcid.org/0000-0001-7615-6632

Protection of external information perimeter of organization from spear phishing

DOI: http://dx.doi.org/10.26583/bit.2018.4.09

Abstract. Spear phishing is one of the social engineering techniques. In case of spear phishing the email text is compiled taking into account the knowledge about a particular company and rather often about the employee using sociology and psychology in such a way that cause the desire to open the attached file or to click on the link. The main difficulty of protection against such e-mails is that the methods of automated analysis do not guarantee its detection, as modern cyber criminals use new text formulations, zero-day vulnerabilities, as well as automation tools to inject exploits into files, which reduces the effectiveness of signature analysis of anti-virus programs. Each of the existing detection technologies alone does not provide protection against spear phishing. However, the combination of technologies (spam filtering, firewalls, anti-viruses), with the mandatory organizational measures, including training and testing of personnel, allows to protect the external information perimeter of the company from the spear phishing. The paper presents a detailed analysis of the technology of spear phishing implemented by two typical methods: the launch of the exploit when clicking on the link and when one runs an executable file. An overview of the vulnerability used in 2016 - 2017 for the attacks is presented. Modern technologies of protection and their comparative analysis are given. It is noted that each of the technologies used separately does not allow an effective protection against spear phishing. On the basis of comparative analysis and analysis of modern information threats the most effective modern methods of protection are proposed.

Keywords: APT, phishing, spearphishing, social engineering, software implementation.

For citation: ZHURIN, Sergey I.; KOMARKOV, Dmitry E. Protection of external information perimeter of organization from spear phishing. IT Security (Russia), [S.l.], v. 25, n. 4, p. 95-107, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1164>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.09.

Введение

В наши дни внешние кибератаки представляют серьезную угрозу для корпоративной среды. Их последствиями могут быть похищенные файлы (пример – Корейская АЭС в 2014 году), нарушение управления производственными процессами (пример, завод по обогащению урана в Натанзе (Иран), вирус Stuxnet в 2009 году).

Кибератаки могут начинаться с поиска оборудования, подключенного к Интернету, например, с использованием открытой платформы SHODAN с последующим подбором пароля или с прослушивания каналов связи, но эти атаки эффективно защищаются простыми мерами, такими как установка сложных паролей и исключение паролей по умолчанию, или шифрацией трафика соответственно. *Наиболее простым способом начала атаки, от которого защититься сложнее, является целевой фишинг.*

По данным компании Group-IB, ежедневно жертвами финансового фишинга в России становятся более 900 клиентов различных банков, что в три раза превышает ежедневное количество жертв от вредоносных программ, а около 10 – 15 % посетителей финансовых фишинговых сайтов вводят на них свои данные [1]. В России, по оценкам Group-IB, действует 15 преступных групп, занимающихся фишингом, направленным на финансовые учреждения [1].

По данным Positive Technologies [2], в 2017 году наиболее популярными являлись кибератаки с использованием вредоносного ПО (39 %), а ущерб от них составил более 1,5 млрд. долл. США. Также в годовом отчете компании отмечается, что одним из главных способов распространения ПО в данном случае являлось фишинговое письмо, использующее методы социальной инженерии.

На данный момент не существует средств защиты информации, которые были бы способны гарантированно детектировать и предотвращать атаки, начинающиеся с целевого фишинга, в котором ставка киберпреступников делается на человеческий фактор, и только технических (программных) средств защиты в этом случае недостаточно. Данная статья направлена на анализ методов целевого фишинга и существующих мер защиты от внедрения

вредоносного ПО в корпоративную среду данным путем. Также приводятся рекомендации по комплексности защиты от целевого фишинга.

1. Целевая атака

Целевые или таргетированные атаки используются для нападения на информационную инфраструктуру компаний [3, 4]. Перед атакой киберпреступники тщательно изучают средства защиты атакуемой организации.

При целевых атаках, как правило, преследуются следующие цели:

- похищение средств с банковских счетов и электронных кошельков [5], а также конфиденциальной, коммерческой информации;
- нечестная конкуренция: манипулирование процессами, подделка документов, ослабление конкурентов, вымогательство и шантаж;
- нарушение нормальной деятельности объектов [3].

Рассмотрим модель жизненного цикла целевой атаки, представленной на рис. 1, которая предложена Лабораторией Касперского.

Основной задачей *подготовки* является поиск цели, сбор о ней достаточно детальной приватной информации, опираясь на которую можно выявить слабые места в инфраструктуре. При этом выстраивается стратегия атаки, подбираются доступные инструменты, либо происходит их самостоятельная разработка.

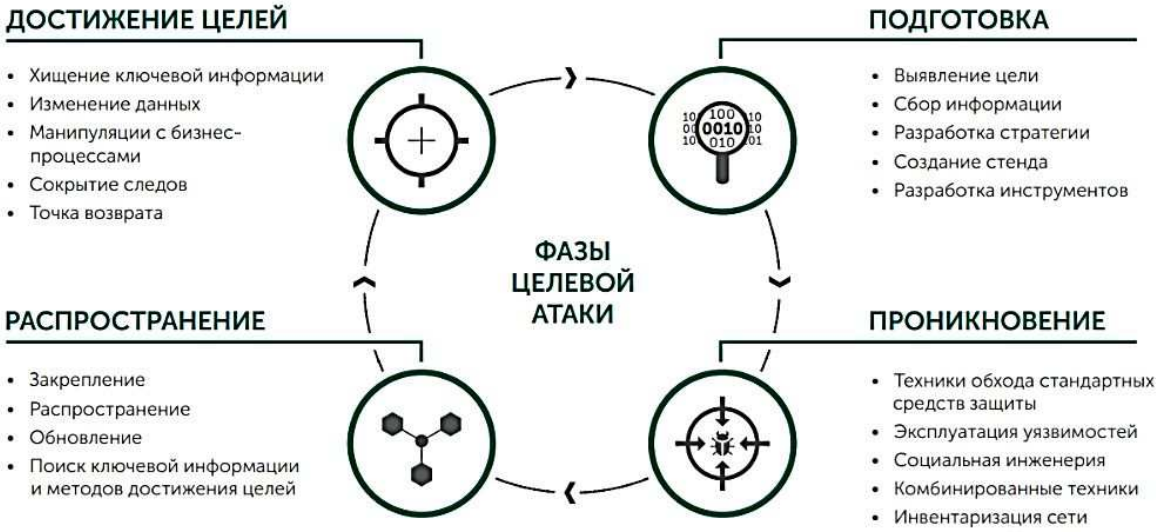

Рис. 1: Фазы целевой атаки

Рис. 1. Жизненный цикл целевой атаки
(Fig. 1. Life-cycle of target attack)

Проникновение – активная фаза целевой атаки, проводимая для первичного инфицирования цели и внутренней разведки. *Здесь широко используется целевой фишинг*. По окончании разведки и после определения принадлежности инфицированной рабочей станции по команде злоумышленника через центр управления загружается дополнительный вредоносный код.

Распространение – фаза закрепления внутри инфраструктуры. Максимально распространяя свой контроль, при необходимости корректируя версии вредоносного кода через центры управления.

Достижение цели – ключевая фаза целевой атаки, в зависимости от выбранной стратегии в ней может применяться хищение или изменение информации, манипуляции с бизнес-процессами компании.

2. Целевой фишинг – элемент целевой атаки

Целью фишинга [6] является получение доступа к конфиденциальным данным пользователей или установка вредоносного ПО с использованием методов социальной инженерии.

Главный инструмент фишинга – электронная почта. На почтовый ящик жертвы злоумышленник отправляет письмо, которое должно побудить его ввести необходимую информацию. Также сообщение может содержать вредоносное вложение, которое при этом проникнет в систему и будет собирать и отправлять информацию злоумышленнику. Особенность классического фишинга – массовая рассылка писем с идентичным содержанием.

Целевой фишинг (англ. spear-phishing), в отличие от обычного [7], направлен на конкретную цель, а значит является намного опаснее, поскольку киберпреступники специально собирают информацию о жертве, чтобы сделать свое послание убедительнее. Качественно сделанное письмо для целевого фишинга иногда очень трудно отличить от вполне легитимного письма, не преследующего зловредных целей. Данные особенности сделали метод одним из наиболее эффективных для проведения целевых атак.

Структура целевой фишинговой атаки показана на рис. 2.

Использование целевого фишинга как способа для проведения целевых атак является одним из самых эффективных. Это связано с тем, что метод использует уязвимости персонала, т.е. человеческий фактор [8]. Человек, как известно, является слабым звеном любой системы, т.к. способен принимать необдуманные и спонтанные решения.

Эксперты Positive Technologies провели исследование [2, 8], в котором рассмотрели влияние методов социальной инженерии на персонал нескольких крупных компаний путем рассылки тестовых писем, имитирующих атаку. В отчете были названы наиболее эффективные фишинговые сценарии (тема письма), статистика которых представлена на рис. 3.

Рис. 2. Структура целевой фишинговой атаки
(Fig. 2. Structure of spear-phishing attack)

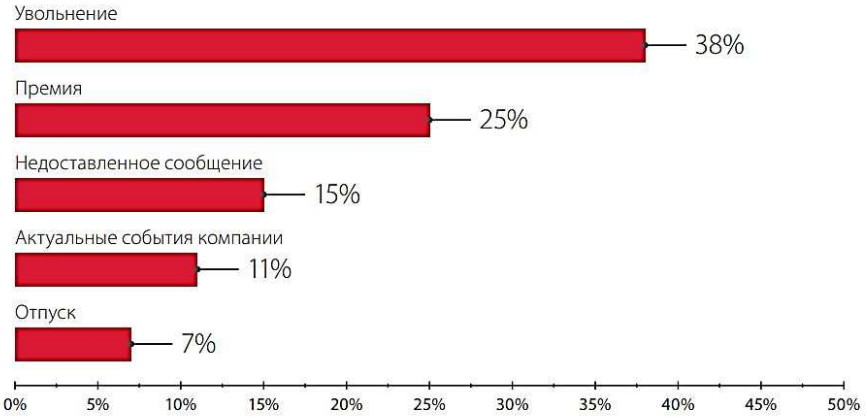

Рис. 3. Темы тестовых писем (доля успешных сценариев)
(Fig. 3. Themes of test letters (the proportion of successful scenarios))

3. Методы внедрения вредоносного кода с использованием целевого фишинга

Существует два типовых метода: вложение и ссылка, которые эксплуатируют уязвимости ПО. **Уязвимостью** программы является ошибка, допущенная программистами на этапе ее разработки. Это и позволяет злоумышленникам получить незаконный доступ к функциям программы или хранящимся в ней данным.

Ошибки могут появиться на любом этапе написания программы, от проектирования до выпуска готового продукта. Причины можно выделить следующие:

- ошибки на этапе проектирования и реализации ПО;
- оставление BackDoor для удаленной отладки;
- применение средств разработки различного происхождения;
- использование в составе ПО сторонних компонентов или свободно распространяемого кода;
- наличие в команде программистов-инсайдеров, которые преднамеренно вносят в написанный код дополнительные функции или элементы.

Любая программа, которая поступает на рынок, имеет уязвимости. И пока они не будут выявлены, разработчик не сможет их устранить. Здесь ключевым моментом является то, кто раньше сможет обнаружить ошибку (*уязвимость нулевого дня)* – сам разработчик или же злоумышленники.

Именно уязвимости нулевого дня используются при проведении целевых атак. Но найти ранее неизвестную уязвимость очень непросто. Поэтому атаки могут проводиться с использованием известных уязвимостей, которые еще совсем недавно стали таковыми. Это осуществимо только тогда, когда потенциальная жертва не установила необходимые обновления, в которых разработчик исправил данную ошибку, и злоумышленнику известна эта информация.

Найденным уязвимостям присваивают код с индексом CVE (Common Vulnerabili-ties and Exposures) с описанием в национальных базах данных, например на сайте ФСТЭК России. Примеры «популярных» уязвимостей [9], [10], [11], [12]:

- CVE-2016-0189 в Windows 10 позволяет удаленным злоумышленникам выполнять произвольный код или вызывать отказ в обслуживании;
- CVE-2016-7200 JavaScript позволяет выполнять произвольный код или вызывать отказ в обслуживании;
- CVE-2015-8651, CVE-2016-4117 –Adobe Flash Player позволяют выполнять произвольный код;
- CVE-2017-0037 в Internet Explorer 11 позволяет выполнять произвольный код.

Эксплойты

Для того, чтобы воспользоваться уязвимостью программы, используют *эксплойты*. Эксплойтом необязательно может быть программа, это может быть небольшой фрагмент вредоносного кода или набор команд, выполняющихся в определенном порядке. Используя уязвимость в какой-либо системной или прикладной программе, эксплойт позволяет получить несанкционированный доступ к приложению или операционной системе и возможность их эксплуатации.

Эксплойты для разных уязвимостей часто упакованы вместе – так, чтобы проверить систему-мишень на широкий спектр уязвимостей. Как только выявляются одна или несколько, в дело вступают соответствующие эксплойты, которые подгружают программы сбора информации об учетных записях пользователей, установленном программном обеспечении, активных процессах и средствах защиты и далее загружают, например, систему удаленного мониторинга, инжектируя вредоносный код в запущенные программы.

В 2017 году злоумышленники использовали в основном недостатки браузеров, но самой популярной среди них оказалась уязвимость, связанная с Microsoft Office.

Средства доставки

Проникнув благодаря уязвимости на целевой корпоративный компьютер, эксплойт запускает средство доставки [2], тип которого зависит от дизайна атаки: это могут быть валидатор, загрузчик или дроппер.

Валидатор является сборщиком данных и выполняет фильтрацию информации об учетных записях пользователей, установленном программном обеспечении, активных процессах и средствах защиты, передает шифрованные данные в центр управления атакой, и, в зависимости от полученной информации, злоумышленником принимается решение о дальнейшем развитии нападения, т.е. выбирается одна из следующих команд:

- загрузка дроппера – приступить к выполнению целевой атаки;
- самоуничтожение – компьютер и данные на нем не представляют ценности для целевой атаки;
- ожидание – решение откладывается, режим «сна».

Обладая минимальным размером и функционалом, валидатор не несет в себе уникальной информации о целевой атаке и ее организаторах, и, если он перехватывается средствами защиты, это не создает для киберпреступников угрозы утечки методов и средств, планируемых к применению.

Дроппер (Dropper) загружает из сети либо выделяет из самого себя компоненты, необходимые для проведения атаки (Payload) с их последующим выполнением. Также его задачей является обход средств защиты и обеспечение скрытности установки.

Загрузчик (Downloader) используется в целях быстрого заражения и при запуске выкачивает основной модуль Payload либо дроппер в зависимости от целей и планов киберпреступников.

Основной модуль *Payload* содержит основные компоненты для проведения атаки и может содержать различные средства сбора информации. Его полная загрузка означает окончание фазы внедрения.

Письмо с вредоносным вложением

Вложением может являться имитация отчета коллеги за предыдущий месяц или сообщение от банка, приславшего пользователю иск за неуплату по кредиту в формате Microsoft Office или *.pdf.

Файлы формата *.pdf часто содержат объекты JavaScript. Поэтому для злоумышленника достаточно просто создать некоторый скрипт, который использовал бы одну из уязвимостей движка от Adobe [13].

В документах Microsoft Office вредоносное ПО может загружаться при помощи макросов, которые содержит файл. При открытии документа исполнение макроса позволяет установить соединение с сервером злоумышленника и начать загрузку. Данная проблема существует довольно давно, поэтому в организациях поддержка макросов отключена по умолчанию. Но если пользователь не осведомлен, то грамотное использование социальной инженерии может заставить его отключить защиту от макросов [13], [14].

На данный момент большинство способов эксплуатации уязвимостей Microsoft Office не требуют использования макросов. Например, используя самую популярную уязвимость 2017 года CVE-2017-0199, при открытии вложенного *.rtf файла можно подгрузить HTA-приложение, поддерживающее исполнение сценариев, со стороннего сервиса и запустить его.

Помимо рассмотренных случаев существует множество других офисных продуктов и форматов, с которыми они работают. Но принцип атаки один и тот же – запустить скрытый сценарий, который позволит загрузить ПО злоумышленника на атакуемый компьютер.

Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и Offensive Ware Multi Exploit Builder (OMEB) [1].

Письмо со ссылкой

В качестве содержания письма также может отправляться ссылка. Целью злоумышленника в данном случае является переход жертвы на определенный веб-ресурс, где, используя уязвимости самого сайта или браузера переходящего, преступник также пытается внедрить зловредное ПО.

Для проведения подобных операций создаются фишинговые сайты, которые живут, как правило, недолго. Они, как правило, являются точными копиями известных сайтов, полностью повторяют их дизайн и структуру. Но они являются лишь копиями, поэтому будут иметь отличающееся от оригиналов доменное имя.

При переходе по ссылке пользователь становится жертвой различных видов XSS-атак. Суть данных атак заключается в выполнении скрипта в браузере и последующем его взаимодействии с сервером злоумышленника. Эти операции позволяют получить доступ к данным браузера и дают возможность применять к нему эксплойты, а также красть cookie, данные авторизации или, например, выполнять HTTP-запросы от имени пользователя.

Мошенники не просто копируют сайт компании или банка, их логотипы и фирменные цвета, контент, контактные данные, регистрируют похожее доменное имя, они еще активно рекламируют свои ресурсы в соцсетях и поисковых системах. Например, пытаются вывести в топы выдачи ссылки на свои фишинговые сайты по запросу [1].

Еще несколько лет назад одного взгляда на адрес было достаточно, чтобы понять, что сайт фишинговый. Однако хакеры научились манипулировать отображением ссылки в адресной строке. В результате пользователь видит адрес, на 100 % совпадающий с официальным. Эта технология называется «спуфинг» (англ. spoofing - обман, мистификация) [1].

Преступники подделывают даже SSL-сертификат – это цифровое удостоверение сайта, которое подтверждает, что обмен данными между сайтом и браузером идет по защищенному каналу. Хакеры используют готовые фишинг-наборы (Phishing kits) – это уже готовый фишинговый сайт с конфигурационным файлом, в котором определяется логика работы фишингового сайта и то, куда должны быть отправлены скомпрометированные данные [1].

4. Анализ существующих мер защиты

4.1 Организационные меры

Фишинг как способ атаки успешен по большей части из-за человеческого фактора [14]. Человек, как известно, является слабым звеном в любой системе. Концентрация лишь на техническом оснащении системы защиты информации является большой ошибкой.

Осведомленность пользователя [14], [15], [16] может существенно повысить уровень защищенности организации.

Во-первых, необходимо минимизировать размещение электронных адресов на открытых сайтах (сайте компании, открытых торговых площадках, личных страницах пользователей и т.п.) и ограничить доступ сотрудников к общей базе данных корпоративных адресов (в качестве примера можно привести известный пример с Эксклектоном, который продал базу данных корпоративных Министерства энергетики для целевого фишинга).

Во-вторых, для снижения уровня влияния человеческого фактора необходимо предпринять следующие меры:

- регламентирование политики использования корпоративной почты;
- обучение персонала;
- проведение тестирования.

Политика использования email

Выделим основные принципы такой политики:

- электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей, а не для личных целей;
- все электронные письма являются собственностью организации и не считаются персональными;
- организация может получить доступ к электронной почте сотрудников;
- пользователи не должны позволять кому-либо посылать письма, используя их идентификаторы;
- запрещение использования сторонних почтовых клиентов;
- справочники электронных адресов сотрудников доступны только внутри компании.

Обучение и тестирование персонала

Под обучением понимается повышение осведомленности пользователей. Персонал должен понимать возможности злоумышленников и способы атак, а также постоянно сохранять бдительность. Поэтому необходимо проводить соответствующие семинары и тренинги по темам:

- основные принципы фишинга;
- методы социальной инженерии;
- важность использования последних версий ПО;
- анализ расширений файлов и текста ссылок.

Администратору необходимо постоянно следить за обновлением ПО.

Для оценки подготовленности персонала к целевой атаке, организация может проводить тестирование. Тестирование осуществляется с использованием стандартных имеющихся программ, или со специально созданных почтовых ящиков, с обязательным информированием пользователей о проводимых учениях, за несколько недель до этого.

4.2 Программно-технические меры защиты

Системы фильтрации спама

Фильтрация нежелательных писем является первой ступенью защиты в борьбе с фишингом.

Анализ IP-адреса сервера отправителя

Данный вид анализа направлен на установление репутации IP отправителя, которая осуществляется путем его поиска в «черных списках». Подобная защита эффективна против массового фишинга, но бесполезна при целенаправленной атаке.

Анализ тела письма

Спам-фильтр может проверять содержимое письма: заголовок, тему, текст, ссылки и вложения. В текстовом содержании проверяется наличие словосочетаний, которые наиболее часто применяются при фишинговых методиках. Указанные ссылки при помощи алгоритмов анализируются на предмет схожести с известными ресурсами, а также, как и в случае с IP-адресами, осуществляется поиск доменных имен в списках нежелательных или имеющих подозрительную активность. Соответственно, у вложений проверяются имена и расширения.

SPF/DKIM-анализ

SPF является расширением для протокола отправки электронной почты, который позволяет получателям проверять IP-адрес отправителя с помощью просмотра списка авторизованных шлюзов для определенного домена в DNS-записях. То есть благодаря SPF можно проверить, не подделано ли доменное имя отправителя и является ли легитимным. Агенты передачи почты, получающие почтовые сообщения, могут запрашивать SPF-информацию с помощью DNS-запроса, верифицируя таким образом сервер отправителя.

DKIM является методом email аутентификации, дающим возможность получателю проверить, что письмо действительно было отправлено с заявленного домена. Вместо традиционного IP-адреса для определения отправителя сообщения DKIM добавляет в него цифровую подпись, связанную с именем домена организации. Подпись автоматически проверяется на стороне получателя, после чего, для определения репутации отправителя, применяются «белые списки» и «чёрные списки».

Использование данных технологий защищает от IP-спуфинга и подмены имен, что в значительной мере препятствуют массовому фишингу, но не защищает от целевого.

Межсетевые экраны

Межсетевой экран осуществляет контроль и фильтрацию проходящего через него сетевого трафика с использованием ряда правил. Работа экрана может осуществляться как на сетевом, так и на транспортном уровне и заключается в анализе заголовков пакетов.

При анализе заголовка сетевого пакета могут использоваться следующие параметры:

- IP-адреса источника и получателя;
- тип транспортного протокола;
- поля служебных заголовков протоколов сетевого и транспортного уровней;
- порт источника и получателя.

Межсетевой экран обычно используется в совокупности с другими средствами защиты информации, где его практическая значимость возрастает. Но в отдельности он не способен противостоять сложным и заранее продуманным атакам.

Антивирусные решения

Современные антивирусные решения включают в себя: сетевые экраны и спам-фильтры, работающие по тем же принципам, которые были описаны ранее. А также проводят анализ загружаемого или работающего ПО с использованием следующих методов:

- сигнатурный анализ;
- эвристический анализ;
- песочница.

Сигнатурный анализ детектирует только ранее известное вредоносное ПО. При этом файлы даже со старой инжектированной системой, удаленной мониторинга, могут быть не идентифицированы, особенно при инжектировании в новый файл. Эвристический анализ может выявить новое вредоносное ПО, однако при этом высок процент ошибки, что может потребовать время на дополнительный анализ. Песочница позволяет более эффективно

идентифицировать такое ПО, например, загрузчики вредоносного ПО, например, перемещая время вперед и имитируя загрузку разных систем, браузеров.

IDS/IPS

Система обнаружения вторжений (IDS), как и система предотвращения вторжений (IPS), является программным или программно-аппаратным средством защиты информации. Данные системы предназначены для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими, и одним из требований к данным системам является обнаружение активности вредоносного ПО.

IDS производит поиск злонамеренных файлов сигнатурным анализом, а значит эксплуатация уязвимостей нулевого дня скорее всего останется незамеченной. Отличие IPS заключается в том, что данная система ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника, а значит более полезна в обеспечении безопасности.

Данные системы, в отличие от рассматриваемых ранее, имеют подсистему анализа данных, а значит обладают преимуществом, поскольку способны вести наблюдение за пользовательской активностью, а также выявлять аномальное поведение файлов, сообщая об этом администратору.

UTM-системы

Система UTM является комплексным решением и содержит:

- межсетевой экран;
- фильтр URL;
- антивирусное решение;
- спам-фильтры;
- IDS/IPS.

Все составляющие системы работают по ранее описанным принципам, но оптимизация их взаимодействия способна улучшить показатели по детектированию угроз.

Использование подобных решений для компании вытекает в ряд положительных моментов, таких как простота настройки и обеспечения системы безопасности, а также простота обучения персонала и уменьшение затрат на защиту.

Системы защиты конечных точек

EDR-системы разработаны для предотвращения атак со сложной структурой. Платформа EDR не просто защищает компьютерную систему от вредоносных тел, она умеет моментально замечать новейшие угрозы высокой сложности и одновременно проявлять реакцию на возникшую ситуацию. Под конечной точкой в данном случае подразумевается рабочая станция, сервер или любое другое компьютерное устройство.

С учетом того, что данные системы имеют достаточно сложное устройство, они, как правило, способны взаимодействовать с другими системами защиты, такими как SIEM.

Работа платформы EDR начинается с установки агента на компьютерное устройство пользователя (конечную точку). Затем осуществляется анализ действий приложений, запускаемого на компьютере, полученные данные отправляются в облако. Защитное решение способно классифицировать практически все приложения, по которым поступает информация, в том числе программы с вредоносным кодом и без него.

Основным компонентом подобных решений является система обнаружения таргетированной атаки, которая имеет:

- сетевые/почтовые сенсоры, позволяющие осуществлять сбор информации с различных контрольных точек;
- сенсоры рабочих станций, позволяющие увеличить охват и детализацию анализируемой информации;

- компонент динамического анализа объектов;
- центр по анализу аномалий – создание типовых шаблонов поведения и контроль отклонений от них;
- облачный репутационный сервис – обновляемая в реальном времени база знаний об угрозах, в том числе и по компонентам таргетированных атак.

Важным звеном EDR является анализатор аномалий, работа которого основывается на статистическом анализе информации, учитывающем частоту событий и их последовательность. Каналами сбора информации являются сетевые сенсоры и сенсоры рабочих станций. В процессе работы технологии формируется поведенческая модель, отклонение от которой может быть признаком вредоносной активности.

5. Оценка эффективности методов защиты

Как показал анализ, по отдельности средства защиты практически не способны противостоять внедрению вредоносного кода в корпоративную сеть. Следовательно, построение системы безопасности требует комплексного использования различных устройств и техник.

На основе проделанных исследований была проведена оценка эффективности средств защиты. Методы внедрения в данной схеме делятся по разным категориям, поэтому ее практическая ценность заключается в возможности оценки различных видов целевых атак путем усреднения значений. Например, UTM-система обладает средней эффективностью в борьбе с целевой атакой, которая использует фишинговое письмо со ссылкой, переход по которой позволит эксплойту для браузера использовать известную уязвимость и напрямую загрузить payload.

Организационные меры, по сути, не являются средством защиты информации, но их высокая эффективность против фишинга не позволяет не обратить на них внимание.

Экспертная оценка эффективности мер защиты представлена на рис. 4.

Эффективным решением для организации безопасности является внедрение системы защиты конечных точек как более эффективного средства защиты от внедрения ПО при целевых фишинговых атаках. Но данные системы имеют высокую стоимость и относительно сложную процедуру установки, а также требуют высококвалифицированного персонала, поэтому не все организации могут использовать их. Выходом из ситуации является выделение значительных усилий на введение организационных мер, а также использование средств защиты различного характера, т.к. только всесторонняя и комплексная защита способна оказывать противодействие данным атакам.

Если внедрение системы защиты конечных точек по ряду причин не может быть реализовано, то для построения системы защиты корпоративной сети вместе с внедрением организационных мер рекомендуется использовать UTM-системы ввиду простоты эксплуатации, а также потому, что совместно функционирующие спам-фильтры, межсетевой экран и антивирус хоть и не могут противостоять сложным фишинговым атакам, но способны защитить организацию от большинства менее качественно спланированных внедрений.

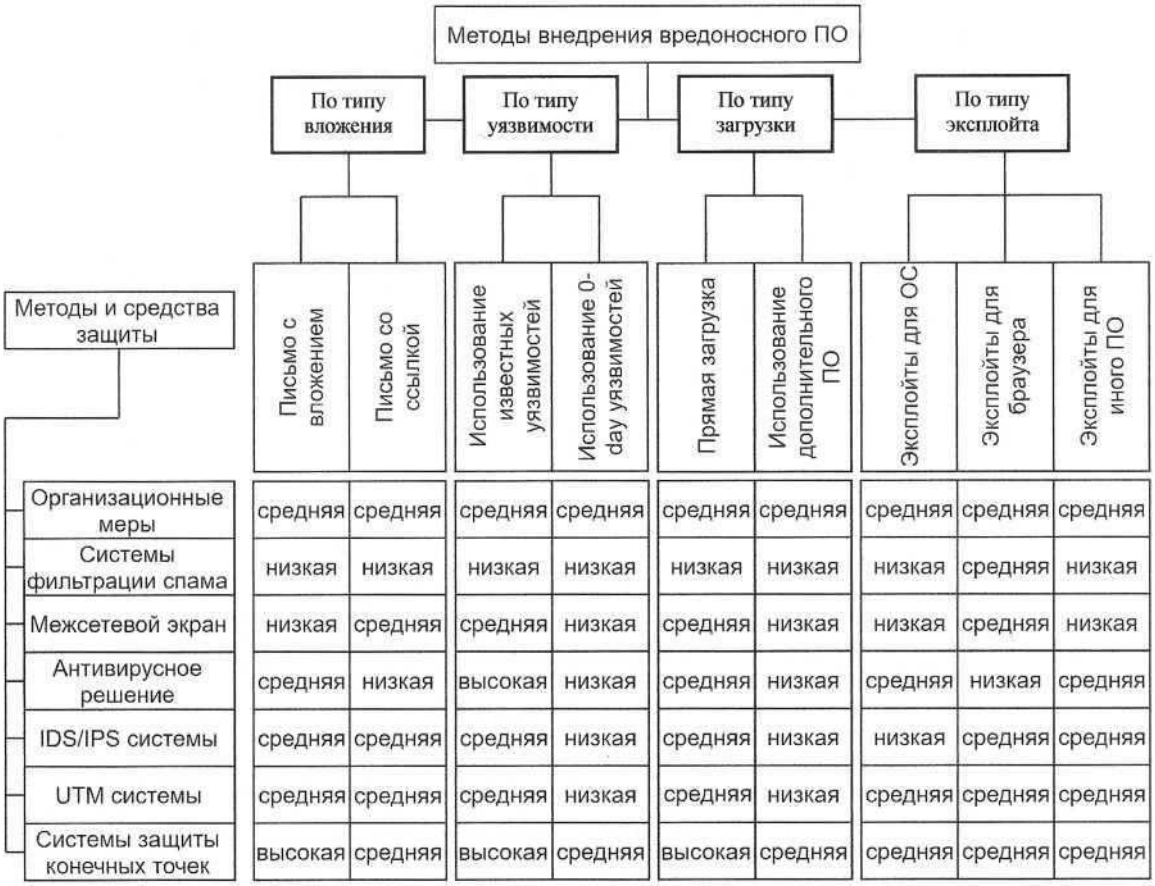

Рис. 4. Экспертная оценка эффективности мер защиты
(Fig. 4. Effectiveness of protection measures)

В табл. 1 представлена экспертная оценка эффективности и сложности внедрения мер защиты. Организационные меры, как видно, имеют наибольшую сложность внедрения.

Таблица 1. Экспертная оценка эффективности и сложности внедрения мер защиты

	Эффективность (в порядке убывания)	**Сложность внедрения (в порядке возрастания)**
1	Системы защиты конечных точек	Антивирусные решения
2	Организационные меры	Системы фильтрации спама
3	UTM системы	Межсетевые экраны
4	IPS/IDS системы	UTM системы
5	Антивирусные решения	IPS/IDS системы
6	Межсетевые экраны	Системы защиты конечных точек
7	Системы фильтрации спама	Организационные меры

Заключение

В целом был проведен анализ существующих методов и средств защиты, в результате которого произведена оценка их способности противостоять современным методам внедрения вредоносного ПО, после чего даны рекомендации по построению

эффективной системы защиты. Приведенные рекомендации помогут выбрать меры защиты от целевого фишинга при проектировании защиты внешнего периметра организации.

В будущих исследованиях планируется исследование, сравнение и апробация программ для тестирования устойчивости к целевому фишингу (например, Gophish или SendPulse), а также более подробное исследование применяемых для фишинга уязвимостей.

СПИСОК ЛИТЕРАТУРЫ:

1. High-Tech Crime Trends 2017 [Электронный ресурс] // Отчет Group-IB. – Режим доступа к ресурсу URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
2. Актуальные киберугрозы 2017 года [Электронный ресурс] // Отчет Positive Technologies. – Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (дата обращения: 14.03.18).
3. Meicong Li, Wei Huang. The Study of APT Attack Stage Model [Электронный ресурс]. – Режим доступа к ресурсу URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (дата обращения: 18.03.18).
4. Анатомия таргетированной атаки [Электронный ресурс] // KasperskyLab. – Режим доступа к ресурсу URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 15.03.18).
5. B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges [Электронный ресурс]. //— Режим доступа к ресурсу URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (дата обращения: 25.03.18).
6. Spear-Phishing Attaks. Why they are successful and how to stop them. [Электронный ресурс] // Отчет FireEye.– Режим доступа к ресурсу URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (дата обращения: 25.03.18).
7. Как социальная инженерия открывает хакеру двери в вашу организацию. [Электронный ресурс] // Отчет Positive Technologies. – Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (дата обращения: 16.04.2018).
8. Актуальные киберугрозы 2017 – Тренды и прогнозы [Электронный ресурс] // Отчет Positive Technologies.– Режим доступа к ресурсу URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (дата обращения: 15.03.18).
9. Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks [Электронный ресурс]. — Режим доступа к ресурсу URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (дата обращения: 16.04.2018).
10. Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. [Электронный ресурс] // Отчет Recorded Future. — Режим доступа к ресурсу URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (дата обращения: 16.04.2018).
11. Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. [Электронный ресурс] // Отчет Recorded Future.– Режим доступа к ресурсу URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (дата обращения: 16.04.2018).
12. New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016. [Электронный ресурс] // Отчет Recorded Future. – Режим доступа к ресурсу URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (дата обращения: 16.04.2018).
13. Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing [Электронный ресурс]. – Режим доступа к ресурсу URL: https://dl.acm.org/citation.cfm?id=3025831(дата обращения: 16.04.2018).
14. Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks [Электронный ресурс]. – Режим доступа к ресурсу URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (датаобращения: 16.04.2018).
15. Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., Vol. 8, No. 3, 2015, p. 230 – 248.
16. Журин С.И. Основы противодействия инсайдерским угрозам. Учебное пособие. МИФИ 2014. 262 стр.

REFERENCES:
[1] High-Tech Crime Trends 2017. Group-IB Report. – URL: https://www.group-ib.ru/resources/threat-research/2017-report.html. (Accessed: 18.03.18).
[2] Topical Cyber-threats 2017. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/webinar_290218.pdf (Accessed: 14.03.18).
[3] Meicong Li, Wei Huang. The Study of APT Attack Stage Model. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7550947&tag=1 (Accessed: 18.03.18).
[4] Targeted Attack Anatomy. Kaspersky Lab. — URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (Accessed: 15.03.18). (in Russian).
[5] B. B. Gupta, Aakanksha Tewari. Fighting against phishing attacks: state of the art and future challenges. – URL: https://link.springer.com/content/pdf/10.1007%2Fs00521-016-2275-y.pdf (Accessed: 25.03.18).
[6] Spear-Phishing Attacks. Why they are successful and how to stop them. FireEye Report. – URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (Accessed: 25.03.18).
[7] How social engineering opens a door to your organization. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf (Accessed: 16.04.2018). (in Russian).
[8] Topical Cyberthreats 2017— Trends and forecasts. Positive Technologies Report. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (Accessed: 15.03.18). (in Russian).
[9] Tzipora Halevi, Nasir Memon, Oded Nov. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742 (Accessed: 16.04.2018).
[10] Scott Donnelly. Soft Target: The Top 10 Vulnerabilities Used by Cybercriminals. RecordedFuture Report. – URL: https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf (Accessed: 16.04.2018).
[11] Gone in a Flash: Top 10 Vulnerabilities Used by Exploit Kits. RecordedFuture Report. — URL: https://www.recordedfuture.com/top-vulnerabilities-2015/ (Accessed: 16.04.2018).
[12] New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.] Recorded Future Report. – URL: https://www.recordedfuture.com/top-vulnerabilities-2016/ (Accessed: 16.04.2018).
[13] Daniela Oliveira Harold Rocha Huizi Yang. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. – URL: https://dl.acm.org/citation.cfm?id=3025831(Accessed: 16.04.2018).
[14] Thomas, J. E. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171727 (Accessed: 16.04.2018).
[15] Zhurin S.I., Comprehensiveness of Response to Internal Cyber-Threat and Selection of Methods to Identify the Insider. ICT Res. Appl., Vol. 8, No. 3, 2015, p. 230 – 248.
[16] Zhurin S.I. Basics of countermesuares against insider threats. Tutorial for students. MEPhI, 2014. p. 262.

Поступила в редакцию –07 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received –August 07, 2018. The final version – November 01, 2018.