



POSITIVE TECHNOLOGIES

**Взломать
любой ценой**

Сколько может стоить АРТ

Содержание

Введение.....	2
Резюме.....	3
Об исследовании.....	3
Инструменты АРТ	4
На этапе проникновения.....	4
В ходе развития атаки	8
Сколько может стоить АРТ.....	13
Выводы и рекомендации.....	15

Г Введение

Активы перспективных коммерческих компаний и государственных структур всегда были и будут привлекательной целью для злоумышленников. Крупные организации, как правило, понимают это и выделяют немало ресурсов на обеспечение информационной безопасности. Так, по результатам нашего исследования, бюджет на ИБ в ряде государственных учреждений достигает 800 млн рублей в год, а по прогнозам Gartner, общемировые затраты на информационную безопасность в 2019 году достигнут отметки в 124 млрд долл. США. Но злоумышленники редко оставляют надежду атаковать выбранную цель даже в случае неудачных попыток. По статистике FireEye, 64% исследованных в 2018 году компаний, которые однажды подверглись атаке, были атакованы повторно в течение 19 месяцев.

Кибератака на компанию с хорошо организованной системой защиты требует специальных знаний и инструментов, а также больших финансовых и временных затрат. Многоэтапные, тщательно спланированные и организованные кибератаки, направленные на отдельную отрасль или конкретные, как правило крупные, компании, называют *advanced persistent threats* (APT). Для проведения таких атак киберпреступники объединяются в преступные группы, которые принято называть АРТ-группировками.

Обнаружить АРТ в момент ее проведения крайне сложно. А закрепившись в инфраструктуре, группировка может оставаться незамеченной в системе годами. К примеру, в компании Bayer специалисты по кибербезопасности наблюдали активность вредоносного ПО в течение года. Самое длительное время присутствия злоумышленников в системе, зафиксированное специалистами экспертного центра безопасности Positive Technologies (PT Expert Security Center, PT ESC), составляет более 8 лет. В то же время, если речь идет о финансово мотивированных атаках, киберпреступная группа предпочитает действовать быстро. Так, всего за три дня АРТ-группировка Lazarus вывела со счета банка Cosmos Bank около 13,5 млн долл. США. Другими словами, цель кибератаки может диктовать модель поведения преступников, техники, которыми они будут пользоваться, и инструменты, которые станут применять.

В данном исследовании мы постараемся оценить, сколько стоят инструменты, которые используются сегодня для АРТ, и как легко их достать. Кроме того, мы выясним, как именно цель атаки влияет на используемые инструменты. Возможно, выводы, сделанные в данном отчете, помогут специалистам по ИБ сфокусировать свое внимание на защите ключевых систем с учетом специфики атак на компании именно их отрасли.

Резюме



Расчет точной стоимости АРТ не представляется возможным по ряду причин, в частности из-за сложной оценки стоимости уникального ПО из арсенала группировки. Все приведенные в данном отчете суммы являются оценочными, реальные затраты на АРТ могут быть существенно выше

- Фишинговые рассылки — эффективный способ проникновения во внутреннюю сеть компании, сегодня к нему прибегают 90% АРТ-группировок. Общая стоимость инструментов для создания вредоносных вложений без учета стоимости эксплойтов для уязвимостей нулевого дня составляет порядка 2 тыс. долл. США.
- Каждая вторая действующая АРТ-группировка после проникновения во внутреннюю сеть использует легитимные инструменты для администрирования и коммерческие инструменты для тестов на проникновение, цена на которые варьируется от 8 до 40 тыс. долл. США.
- Набор инструментов для проведения атаки, направленной на кражу денег из банка, по нашим примерным подсчетам, может стоить от 55 тыс. долл. США. Кибершпионская кампания обходится на порядок дороже, ее минимальный бюджет составляет 500 тыс. долл. США.

Об исследовании

В данном исследовании мы проанализировали инструменты 29 АРТ-группировок, которые действуют в различных странах мира, наиболее активны на протяжении последних двух лет и представляют угрозу для ключевых отраслей — государственного сектора, кредитно-финансовых организаций и промышленности.

Данные для анализа основаны на результатах наших расследований киберинцидентов и работ по ретроспективному анализу событий безопасности в инфраструктуре компаний, а также на результатах постоянного отслеживания активности действующих сегодня АРТ-группировок экспертами PT ESC. Кроме того, дополнительно использовалась информация из общедоступных отчетов о деятельности АРТ-группировок, подготовленных ведущими компаниями в области ИБ.

Мы выделили две основные категории группировок в зависимости от мотива атак — финансово мотивированные (атакующие банки и другие организации с целью кражи денег) и шпионские (атакующие с целью получения ценных сведений и долгосрочного контроля над инфраструктурой).

Инструменты для проникновения в локальную сеть компании отличаются от инструментов, которые используются на последующих этапах в ходе развития атаки. В то же время на стадиях закрепления и дальнейшего перемещения набор инструментов схож. Таким образом, для целей исследования мы разделили инструменты АРТ на две группы:

- для проникновения в локальную сеть,
- для дальнейшего развития атаки во внутренней сети.

Мы проанализировали публикации на 190 площадках в дарквебе, где представлены предложения по покупке и продаже некоторых инструментов, используемых в АРТ, а также объявления о заказной разработке вредоносного ПО. В числе исследованных теневых ресурсов форумы, специализированные маркетплейсы и чаты преимущественно с русско- и англоговорящей аудиторией. Средняя общая посещаемость исследованных ресурсов дарквеба составляет более 70 млн человек в месяц.

Инструменты АРТ

На этапе проникновения

57%

региональных компаний в 2018
году столкнулись с фишингом
в адрес сотрудников



**Фишинг — основной
способ проникновения
в инфраструктуру
компании**

90%

актуальных на сегодня
группировок используют фишинг
на этапе проникновения

Примеры группировок:

Cobalt, APT29, Lazarus

Финансовые затраты на этапе проникновения определяются выбранным способом доставки вредоносного ПО в инфраструктуру компании, а выбор способа зависит от мотивов преступников и степени защищенности потенциальной жертвы.

Главным инструментом финансово мотивированных злоумышленников является фишинг. Для фишинговой рассылки злоумышленнику необходимо подготовить документ, содержащий вредоносное ПО, и лодер (дроппер).

Документы, содержащие вредоносный код, могут создаваться с помощью специальных программ — эксплойт-билдеров. Они позволяют сформировать файл, при открытии которого будет выполняться вредоносный код. Задачей этого кода является загрузка и запуск лодера — небольшой программы, которая подгружает на компьютер основной модуль вредоносного ПО. Лодер, как правило, применяется единожды, так как последующие запуски даже обфусцированного лодера могут быть обнаружены антивирусными средствами.



Рисунок 1. Упрощенная схема подготовки и доставки вредоносного ПО в локальную сеть с помощью фишинга

На стоимость инструментов для создания вредоносных документов непосредственно влияет способность зловредов оставаться незамеченными для антивирусов. К примеру, разработчик сервиса Supremacy обещает, что вредоносный файл не будет детектироваться средствами защиты в течение 2–3 недель, и предлагает покупателям услугу регулярной «очистки» кода, чтобы минимизировать вероятность обнаружения для новых файлов.

2500 \$

стоимость месячной подписки
на сервис по созданию документов
с вредоносным содержимым

Supremacy - office macro (.doc .xls) + exe

malware, эксплойты, связки, АЗ, крипт

3 апреля

Supremacy - выбор профессионалов для таргетированной работы. Идеально подходит для тех случаев когда у Вас есть только электронная почта и одна попытка. На данный момент по прохождению файла через аттач продукт аналогов не имеет.

Описание:

Любые форматы офис поддерживающие макросы.

Работает на всех версиях MS Office и Windows.

FUD Runtime/scantime.

Обход AMSI.

Работает с .exe файлами скачиваемыми с ваших ссылок.

Цены:

2500\$ месячная подписка, до 30 отправок в день. Чистки не реже раза в неделю. 10 мест.

Для участников подписки, бесплатная разработка СИ шаблонов с графикой под Ваши задачи. Есть богатый опыт создания СИ шаблонов. Перепродажа запрещена для индивидуального пользования.

Разовый билд для теста 150\$ (только таргет) когда наберется 10 человек на подписку услуга будет закрыта.

Рисунок 2. Предложение услуг по созданию фишинговых рассылок

От 300 \$

стоимость инструмента
для создания вредоносных файлов

Готовый лoader можно приобрести всего за 25 долларов, а вот за исходный код придется заплатить уже от 1500 долларов, при этом на последующую доработку тоже понадобятся дополнительное время и деньги.

Продажа JS лoaderов/дроперов

Ответить в тему

« НАЗАД Страница 1 из 5 ВПЕРЕД »

Минимальный разовый заказ - 25-30\$ - состоит из 1-5 билдов JS лoaderа по одной или несколько ссылок на каждый, или же из криптоа предоставленного Вами файла. Ссылки в билдах ставятся одинаковые, код на выходе - разный. Дропер в отличие от лoaderа содержит не линк, а Ваш exe файл целиком. Если Вам требуется больше 5 билдов и/или билды с разными ссылками - цена может быть немного выше.

- работаю собственным JS криптором/обфускатором;
- лoaderы/дроперы протестированы на Windows XP, 7, 10;
- ScanTime FUD + ручной тест на Avast, ESET, Windows Defender.

Также имеются свои VBS и CMD/BAT обфускаторы, и лoaderы этих форматов.

На данном этапе сосредоточен на разовых заказах, которые делаю в полуручном режиме путём обфускации кода в несколько проходов, что обеспечивает наиболее оптимальную живучесть при небольших затратах с Вашей стороны.

Рисунок 3. Объявление о продаже готовых лoaderов

От 1500 \$

стоимость исходного
кода лодера

продам сорци лодыря писался когда то для себя, язык С , вес без сжатия 40 - 50 кб
фикции дроп диск , загрузка в память ехе , длл , файллесс,
софтец устал немного надо чистить

продажа только гарант этого форума либо эксп
цена 1500\$
чистка и доработка обсуждается в пм

Рисунок 4. Продажа исходного кода лодера

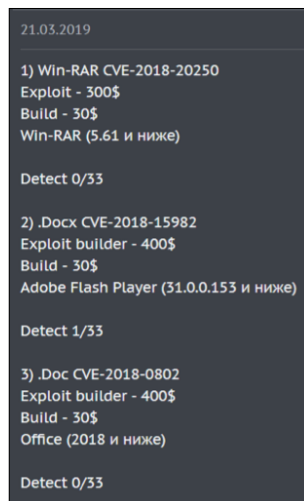


Рисунок 5. Объявление
о продаже эксплойт-билдеров

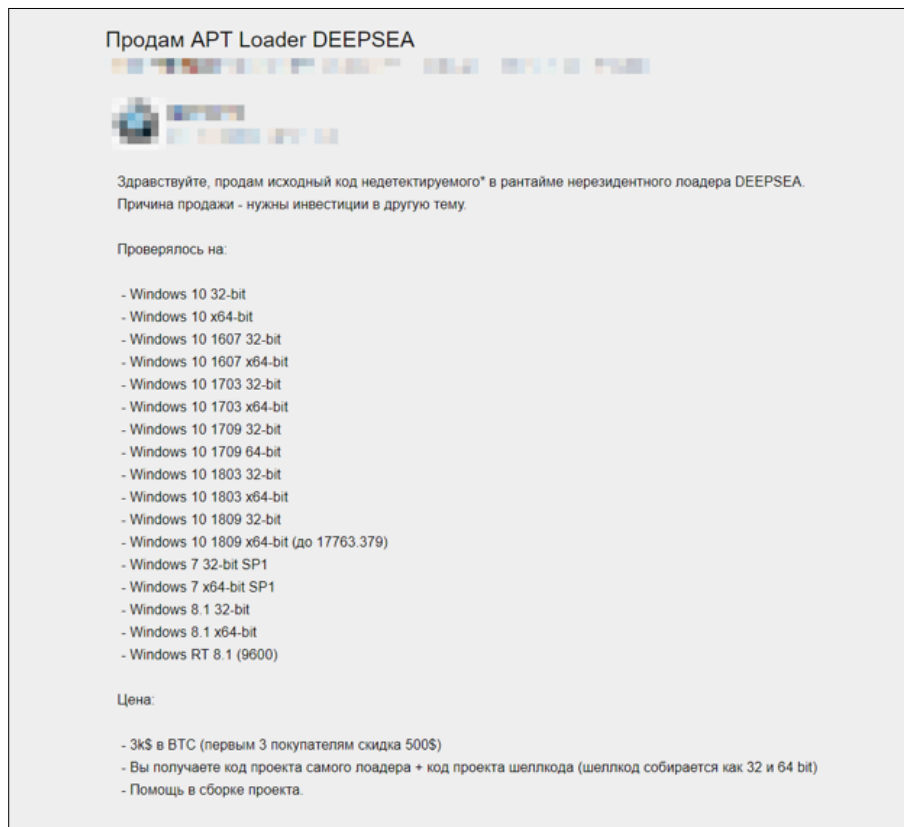


Рисунок 6. Продажа исходного кода лодера DEEPSEA

Рассылку фишинговых писем активно эксплуатирует группировка Cobalt. Эта группа постоянно совершенствует свои техники и использует актуальные уязвимости. В 2017 году группировка Cobalt получила эксплойт-билдер для уязвимости CVE-2017-0199, который на тот момент продавался за 10 тыс. долларов. Сейчас цены на эксплойт-билдеры для этой уязвимости уже намного ниже и их можно приобрести всего за 400 долларов.

10 000 \$

стоимость эксплойт-билдера,
который использовала
группировка Cobalt



Рисунок 7. Объявление о продаже эксплойт-билдера для CVE-2017-0199 в мае 2017 года

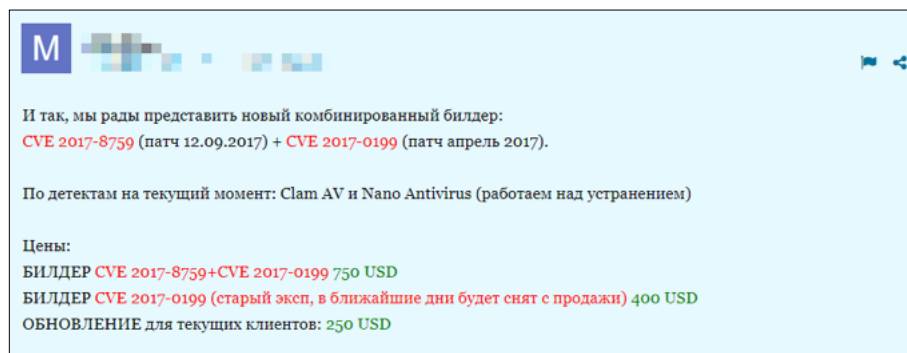


Рисунок 8. Актуальные цены на эксплойты для уязвимостей 2017 года

Топ-5 уязвимостей, эксплуатируемых АРТ-группировками в 2018 году:

CVE-2017-0199,
CVE-2017-11882,
CVE-2018-0802,
CVE-2016-7255,
CVE-2018-8174

Финансово мотивированная группировка Silence также использует фишинг в качестве инструмента для проникновения, эксплуатируя ряд уязвимостей, в частности [CVE-2018-0802](#), [CVE-2018-8174](#). Цена за набор эксплойтов для этих уязвимостей на теневом рынке киберуслуг начинается от 1600 долларов.

Преступникам, действующим из финансовых побуждений, важен быстрый результат (обычно время с момента рассылки писем до вывода денег составляет от недели до месяца), поэтому они охотно покупают готовые инструменты и проводят массовые фишинговые рассылки.

Как и в случае с финансово мотивированными атаками, шпионские АРТ чаще всего начинаются с фишинговых писем. Однако если фишинг злоумышленников, которые хотят украсть деньги, может быть направлен на отрасль в целом, то кибершпионы действуют точно и наверняка, тщательно готовятся. Например, шпионская группировка [SongXY](#), деятельность которой расследовали специалисты РТ ESC, во время очередной попытки проникновения рассылала документ со ссылкой на изображение, размещенное на контрольном сервере. Ссылка срабатывала автоматически при открытии документа. Это позволяло хакерам собирать дополнительную информацию о конфигурации серверов, в том числе о версии Microsoft Office, и подбирать вредоносный документ с необходимым для компрометации системы эксплойтом.

Эксплойт-билдеры и лодеры, которые используют кибершпионы, не продаются в дарквебе. Даже примерно оценить, сколько могли бы стоить такие инструменты, крайне сложно. Можно лишь сравнить их стоимость с расценками на заказную разработку в дарквебе. По нашим данным, за разработку одного уникального инструмента в соответствии с требованиями заказчика на темных форумах злоумышленники готовы платить 20 тыс. долларов и более.

Шпионские АРТ-группировки могут готовить вредоносные письма и вручную, для них важно, чтобы вредоносный код не был обнаружен ни одной системой безопасности, при этом в первую очередь отрабатывается обход именно тех средств защиты, которые используются в целевой организации. О том, какие средства входят в систему защиты жертвы, злоумышленники могут узнать заранее, на этапе разведки. Текст и стилизация электронных рассылок шпионских группировок хорошо продуманы, поэтому шансы на то, что жертва откроет вредоносное вложение, высокие.

Чтобы максимально увеличить вероятность успеха фишинговой рассылки, кибершпионские АРТ-группировки могут взламывать компании партнеров или подрядчиков целевой организации и рассылать письма от их имени. Весной 2019 года хакеры [проникли](#) в сеть IT-гиганта Wipro и рассылали от его имени фишинговые письма клиентам компании.

14%

группировок используют watering hole на этапе проникновения

Стоимость: от 10 000 \$

Примеры группировок:

APT29, APT35, TEMP.Periscope,
DarkHydrus

Больше 1 млн \$

могут стоить отдельные эксплойты
для уязвимостей нулевого дня

Иногда злоумышленники прибегают к другому типу атаки, который называется watering hole. В ходе этой атаки хакеры определяют веб-ресурсы, которые регулярно посещают сотрудники целевой компании, например это могут быть сайты партнеров или популярные веб-ресурсы определенной отраслевой тематики. Злоумышленники взламывают эти сайты с целью размещения на них вредоносного ПО. Дальнейшее посещение зараженных сайтов сотрудниками целевой компании может закончиться успешным проникновением злоумышленников во внутреннюю сеть.

Кибершпионские группировки обычно не считаются с затратами и могут использовать в атаках дорогостоящие эксплойты для уязвимостей нулевого дня, разрабатывать собственные инструменты, осуществлять атаку в несколько этапов, подбираться к цели через цепочку сторонних организаций.

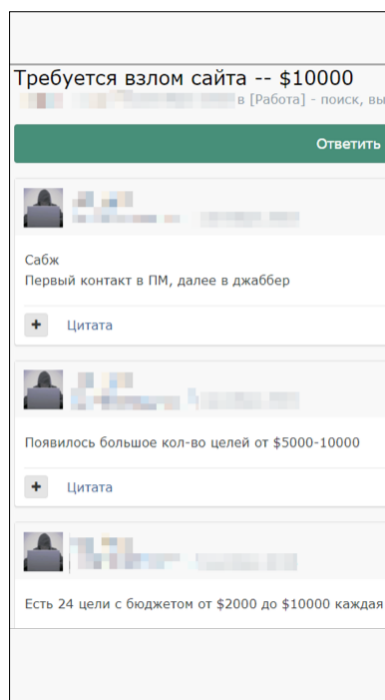


Рисунок 9. Спрос на услугу по взлому сайта на теневом рынке

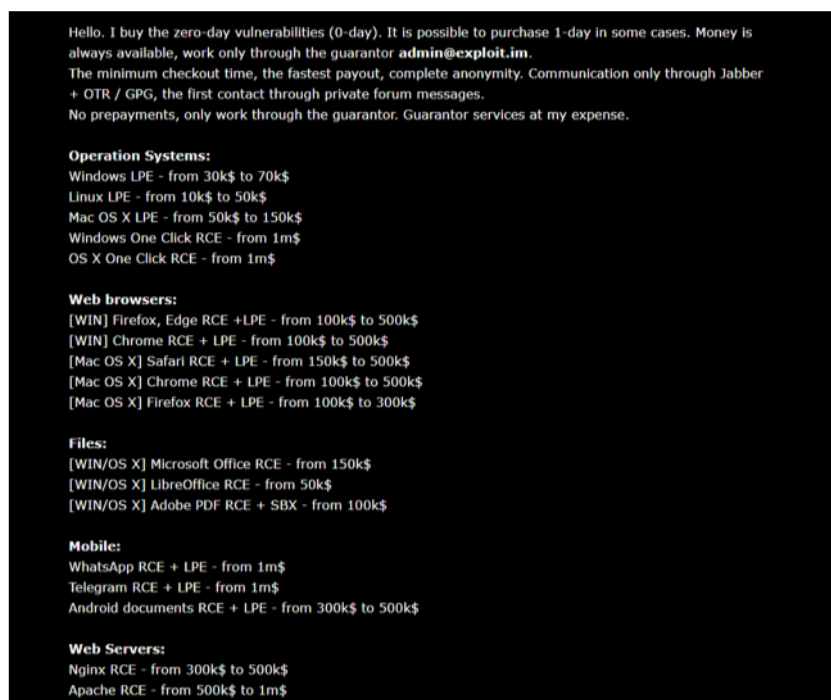


Рисунок 10. Цены, которые готовы платить злоумышленники за уязвимости нулевого дня

В ходе развития атаки

Развитие атаки внутри инфраструктуры компании состоит из множества шагов: выполнение кода на отдельных узлах, повышение привилегий, сбор данных, перемещение между узлами, создание каналов для связи с командным центром. По большей части наборы инструментов различных АРТ-группировок для развития атаки во внутренней сети схожи. И финансово ориентированные злоумышленники, и шпионские группы отдают предпочтение общедоступному легитимному ПО, прибегая к собственным разработкам или покупке утилит на форумах в дарквебе лишь при необходимости.

Cobalt Strike и Metasploit Framework Pro — коммерческое ПО, предназначенное для проведения тестов на проникновение. Однако, кроме специалистов по анализу защищенности, данные инструменты стали использовать и хакеры. Как отмечали специалисты ФинЦЕРТ Банка России, использование инструментов, предназначенных для тестов на проникновение, в финансово мотивированных атаках — тренд

48%

действующих сегодня АРТ-группировок
используют инструменты для
тестирования на проникновение

Cobalt Strike

Официальная цена на момент проведения исследования — 3500 \$ в год

Нелегальные продажи:
30 000—40 000 \$

Группировки:
APT10, APT29, APT32, APT40,
Cobalt, DarkHydrus, Winnti

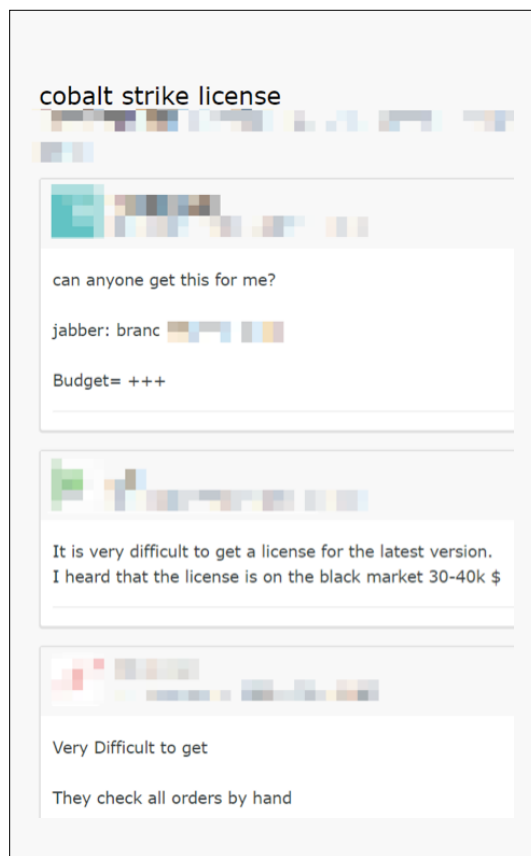


Рисунок 11. Спрос на Cobalt Strike на теневом рынке

2018 года, который распространяется и на 2019 год. Популярность таких инструментов среди хакеров объясняется их удобством, ведь они обладают практически всеми нужными возможностями для проведения атак и, кроме того, регулярно обновляются.

Разработчики Cobalt Strike понимают, что их продукт может использоваться в злонамеренных целях, поэтому проводят строгие проверки компаний — потенциальных заказчиков. Хакеры знают об этом, и периодически на теневых форумах появляется спрос на взломанные или нелегально добытые официальные версии Cobalt Strike.

Metasploit Pro также можно приобрести в дарквебе. На разных площадках представлены не только взломанные оригинальные версии фреймворка, но и модифицированные варианты, в которые добавлены дополнительные функции.

Metasploit Pro

Официальная цена на момент проведения исследования — 15 000 \$ в год

Модифицированная версия с годовой техподдержкой:
8000—15 000 \$

Группировки:
APT35, Carbanak, Patchwork,
Silence, TreasureHunter

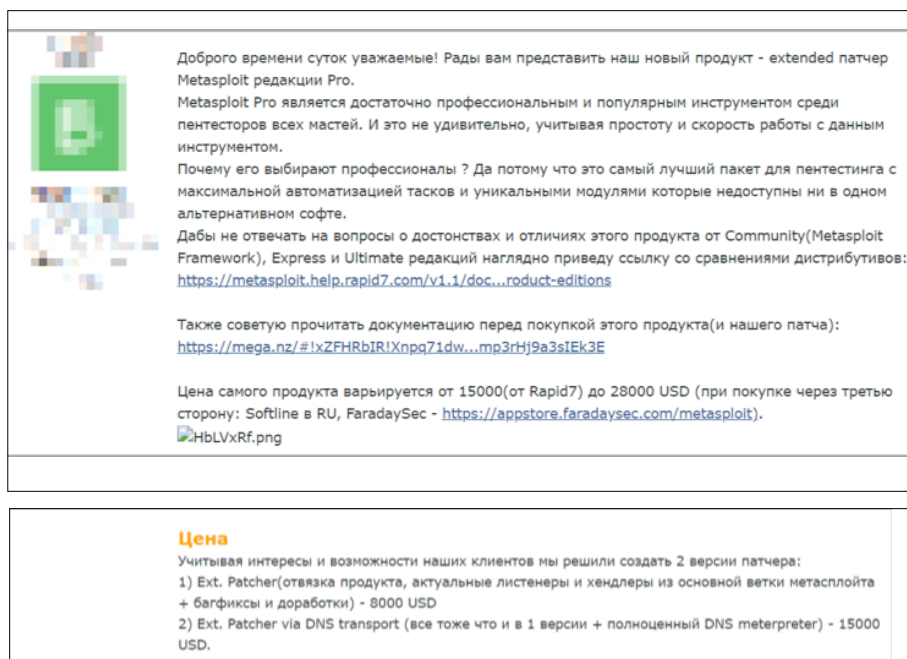


Рисунок 12. Объявление о продаже доработанных версий Metasploit Pro

После проникновения в инфраструктуру финансово мотивированные киберпреступники стараются быстро обнаружить ключевые узлы, например компьютер оператора, который работает с денежными потоками. В банке это может быть АРМ КБР, в коммерческой компании — рабочее место бухгалтера. Для их поиска злоумышленники могут воспользоваться бесплатными утилитами, такими как nmap или nbtscan, но существуют и более удобные коммерческие программы, например группа Cobalt применяла ПО SoftPerfect Network Scanner, официальная стоимость которого составляет 3000 долл. США. Сети крупных организаций сложны и насчитывают огромное количество серверов и рабочих станций, поэтому преступникам важно иметь инструменты, которые позволят легко в подобной сети ориентироваться.

После того как злоумышленники сумели добраться до ключевых узлов, перед ними стоит новая задача — понять принципы работы специализированных банковских программ, а также изучить процессы осуществления операций и их подтверждения. (Если, конечно, преступники заранее обо всем этом не осведомлены.) Принцип работы с АРМ КБР в банках регламентирован, но в коммерческих компаниях могут использоваться одновременно несколько различных банк-клиентов для работы с разными банками. Поэтому хакерам могут понадобиться инструменты, которые позволяют видеть рабочий стол зараженной машины, следить за действиями оператора в реальном времени, делать видеозаписи и скриншоты, при этом сотрудник не должен догадаться, что за ним наблюдают. К такому ПО относятся hVNC, модифицированные версии TeamViewer, RMS, Ammyy Admin и т. п.

TeamViewer

Легитимный инструмент для удаленного администрирования. Модификация незаметна в работе и имеет ряд дополнительных функций, например встроенный кейлоггер

Стоимость в дарквебе: 100 \$

Группировки: Carbanak, Cobalt

Hidden VNC

Модификация легитимной утилиты VNC, позволяет удаленно подключаться к рабочей станции пользователя и незаметно выполнять команды

Стоимость в дарквебе —

1000 \$ в месяц

Используется группировкой Carbanak

Скрытый внц/Hidden vnc

- работает на всех линейках в том же числе серверных ос, от xp до актуального
- яп C/C++
- размер рандом от 200 до 600кб
- стабильный
- рантайм радует

цена:

1к в месяц

выдаю доступ в панель + файлы к нему

Рисунок 13. Объявление о продаже hidden VNC

От 400 \$

стоимость готового банковского бота в дарквебе в базовой комплектации (загрузка и исполнение произвольных файлов)

1750 \$

стоимость банковского бота Smoke Bot с полным набором модулей

[Продаю] Smoke Loader (лоадер + граббер паролей)

Тема в разделе "Софт", создана пользователем [avatar]

Страница 1 из 3 1 2 3 Вперед >

Smoke Bot - новый модульный бот

Здравствуйте, уважаемые форумчане.

Предлагаю Вам собственную разработку:

Smoke Bot

Smoke Bot - это модульный бот (возможны две версии - резидентная и нерезидентная).

* нерезидентная версия - после загрузки, бот выполняет все задания и самоуничтожается, т.е не устанавливается в систему

Преимущества:

- наличие модулей-плагинов, которые расширяют функционал бота, при этом не влияют на размер бота
- подробная статистика по версиям системы, странам и онлайн
- задания для бота на загрузку EXE или DLL (LoadLibrary, regsvr32, запуск из памяти без необходимости в криптовании)
- гео-таргетинг (выборочные загрузки только для конкретных стран или блокировка для определенных стран)
- загрузка задания с удаленного URL
- индивидуальное задание для каждого бота и поиск ботов по ID, стране или префиксу селлера
- незаметная установка в систему, защита собственных файлов и записей в реестре *
- самообновление бота через админку (локально или удаленно) *

SMOKE LOADER

MY BOTNET

SMOKE LOADER is a powerful tool for creating and managing a botnet. It is designed to be stealthy and easy to use. The loader can be configured to download and execute files from a remote server, making it a valuable tool for attackers.

FEATURES:

- **TASK LIST** - View and manage the tasks assigned to your bots.
- **IP LIST** - View the IP addresses of your bots and their status.
- **OPTIONS** - Configure the loader's behavior, such as the download path and the command to execute.
- **GLOBAL GRAB** - Download and execute files from a remote server for all bots.
- **ALSO GRAB** - Download and execute files from a remote server for a specific bot.
- **FILE SEARCH** - Search for files on the infected machine.
- **PROXY** - Use a proxy to hide the loader's origin.

1750\$

Рисунок 14. Объявления о продаже банковского бота Smoke Bot

Sysinternals Suite

Легитимный набор утилит
для администрирования

**Утилиты, наиболее часто
используемые хакерами:**
PsExec, ProcDump, PsList, SDelete

Примеры группировок:

APT29, Leafminer, OilRig

После удачного проникновения во внутреннюю сеть кибершпионы, как и финансово мотивированные киберпреступники, нацелены на закрепление и поиск ключевых узлов. Их интересуют рабочие станции и серверы, на которых хранится и обрабатывается ценная информация — коммерческая тайна или интеллектуальная собственность, а также компьютеры высшего руководства и других ключевых лиц организации или серверы, с которых есть доступ к промышленным сетям с оборудованием АСУ ТП. Прежде чем приступить непосредственно к сбору ценной информации, кибершпионы изучают бизнес-процессы компании. Чтобы не привлекать внимание и не вызывать подозрений, они предпочитают использовать легитимные утилиты администрирования. Например, 48% исследованных нами АРТ-группировок применяют утилиты из бесплатного набора Sysinternals Suite компании Microsoft.

Важным шагом является повышение привилегий в ОС. На теневых форумах продаются эксплойты для повышения привилегий в ОС путем эксплуатации известных уязвимостей или уязвимостей нулевого дня.

10 000 \$

стоимость эксплойта для повышения
привилегий в ОС

Продается ядерный эксплойт для локального повышения привилегий до уровня **SYSTEM**, работающий на всей линейке Windows, защищенной проактивной защитой.

Vulnerability: CVE-2018-8453 (Published: October 9, 2018)
Supported versions:
XP/2003/Vista/2008/W7/2008R2/W8/2012/W8.1/2012R2/W10TH1-RS3/2016
Supported architecture: x86/x64
Development stage: v1.0.81207 (stable)
x86 shellcode size: 13Kb (avg. exec. time: 2-5s)
x64 shellcode size: 19Kb (avg. exec. time: 2-5s)

Обходятся следующие защиты Windows:

- SMEP
- Kernel DEP
- KASLR
- Integrity Level (выход из Low)
- UAC

Цена: 10K USD BTC

ГАРАНТ приветствуется.

Контакты для связи: ██████████

Рисунок 15. Продажа эксплойтов для повышения привилегий

Эксплуатация уязвимостей нулевого дня — характерная черта шпионских группировок, она гарантирует им успешность атаки. Например, группировка TEMP.Reaper использовала уязвимость нулевого дня в Adobe Flash. В настоящий момент брешь имеет идентификатор CVE-2018-4878, а ПО для ее эксплуатации находится в свободном доступе. Еще одна уязвимость нулевого дня (CVE-2018-15982) в Adobe Flash эксплуатировалась в ходе кибершпионской АРТ на российскую государственную поликлинику. Сложно оценить стоимость эксплойта на тот момент, когда об уязвимости еще не было известно. Но мы отмечаем, что стоимость эксплойта для уязвимости нулевого дня в Adobe Acrobat на рынке в дарквебе довольно высокая.

130 000 \$

стоимость эксплойта для уязвимости
нулевого дня в Adobe Acrobat

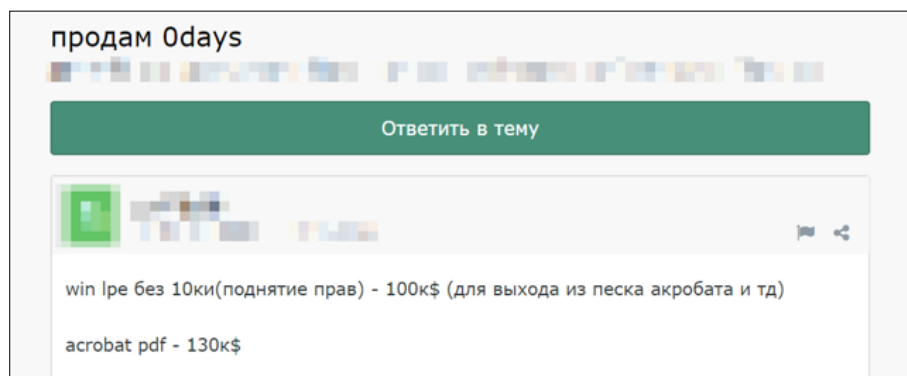


Рисунок 16. Объявление о продаже уязвимостей нулевого дня

1,6 млн \$

стоимость шпионского
фреймворка FinSpy

Уязвимости нулевого дня могут использоваться злоумышленниками для доставки шпионских троянов. Например, в АРТ с использованием уязвимостей нулевого дня в Adobe Flash Player ([CVE-2017-11292](#)) и Microsoft .NET Framework ([CVE-2017-8759](#)) доставлялось ПО FinSpy. Фреймворк FinSpy (также известен под названием FinFisher) — шпионское ПО с возможностью слежки через веб-камеру и микрофон, перехвата сообщений в мессенджерах и почтовом ящике, а также кражи паролей и других чувствительных данных. В настоящее время этот троян использует шпионская АРТ-группировка [SandCat](#). Кроме широких возможностей для кибершпионажа, FinSpy имеет множество механизмов антианализа (обфускация кода, предотвращение запуска в виртуальной машине и др.), что, с одной стороны, затрудняет его обнаружение, и с другой стороны — влияет на стоимость ПО, которая достигает почти полутора миллионов евро.

Для того чтобы обойти механизмы защиты на узлах сети, используются разные техники. К примеру, преступники подписывают вредоносный код с помощью сертификатов, чтобы выдать его за легитимный. Готовые сертификаты также можно найти на специализированных форумах.

1700 \$

стоимость расширенной версии
сертификата для подписи кода

COMODO	Digicert	Symantec
Trust level: basic	Trust level: high	Trust level: maximum
Type: regular	Type: regular	Type: EV certificate
SmartScreen reputation: no	SmartScreen reputation: no	SmartScreen reputation: yes
Must gain a positive reputation to pass SmartScreen filter	Gains SmartScreen reputation faster than Comodo certificates	Contact us for purchase. USB token required (see FAQ)
\$349	\$699	\$1699

Рисунок 17. Реклама услуг по подписи ВПО легитимными сертификатами

Если злоумышленникам требуется доступ в сегменты сети, которые находятся под особой защитой, например в технологические сети, они могут применять инструменты собственной разработки. В рамках вредоносной кампании [TRITON](#), направленной против промышленных предприятий, атакующие применяли собственные средства, в частности программы SecHack для сбора учетных данных и NetExec для продвижения по сети.

Таким образом, стоимость набора инструментов на этапе закрепления и горизонтального перемещения для финансово мотивированной группировки может достигать 30–35 тыс. долл. США. Здесь стоит отметить, что такие затраты группировка несет разово, приобретая готовый комплект ПО, но затем группировка использует один и тот же набор для множества последующих атак, поэтому каждая отдельная атака обходится значительно дешевле.

За эксплойт для одной уязвимости нулевого дня придется заплатить несколько десятков или сотен тысяч долларов. Высокая цена на такие эксплойты не останавливает кибершпионов. Помимо покупки эксплойтов, кибершпионы располагают средствами и для разработки собственного уникального ПО, которое способно обходить антивирусы, выявлять запуск в «песочнице» и т. п. Эти обстоятельства существенно затрудняют обнаружение преступников в инфраструктуре и требуют от атакуемых организаций особых мер и средств для защиты ценной информации; невозможно, в частности, эффективно защититься без высококвалифицированного персонала security operations center, работающего в режиме 24/7.

Сколько может стоить АРТ

При подсчете стоимости АРТ необходимо учитывать не только цену на инструменты для ее проведения, но также множество операционных расходов (аренду серверов, покупку доменного имени, хостинг сайтов, оплату VPN-сервисов и др.). По нашим оценкам, такие расходы составляют порядка тысячи долларов, что существенно меньше стоимости инструментов для атаки. Далее мы дадим экспертную оценку основных затрат киберпреступников на примере нескольких АРТ. Выводы основаны на стоимости аналогичных услуг и ПО, которые предлагаются на теневых площадках в дарквебе.

Г Silence

288 000 \$

средний ущерб от успешной атаки

55 000 \$

стоимость набора инструментов

В начале 2019 года было зафиксировано возобновление активных действий со стороны финансово мотивированной группировки Silence. Попробуем разобраться, сколько могла бы стоить атака этой группировки. Как мы отмечали ранее, месячная подписка на сервис по созданию вредоносных вложений обошлась бы группировке в среднем в 2,5 тыс. долл. США. В ходе атак группировка Silence использует как общедоступное ПО из состава Sysinternals Suite, так и ряд уникальных самописных инструментов; в их числе фреймворк Silence, набор для кражи денег из банкоматов Atmosphere и ряд других. К слову, по результатам нашего отдельного исследования рынка преступных киберуслуг, средняя стоимость готового ВПО для банкоматов составляет около 5 тысяч долларов, и это самый дорогой тип вредоносного ПО в дарквебе. Проанализировав теневой рынок киберуслуг, мы пришли к выводу, что стартовая цена набора инструментов финансово мотивированной АРТ-группировки (такой как Silence) может составить 55 000 долл. США.

Г Атака на ПИР Банк

930 000 \$

ущерб от атаки

66 000 \$

стоимость набора инструментов

В июле 2018 года стало известно об атаке на ПИР Банк, в результате которой финансовая организация потеряла 58 млн рублей. Посчитаем, во сколько могла обойтись подобная атака злоумышленникам. На этапе проникновения преступники использовали фишинговые письма. В их арсенале было собственное ПО, однако во время продвижения по сети они также активно использовали Metasploit Pro и утилиты из пакета Sysinternals Suite. Для наблюдения за сотрудниками банка они применяли инструменты собственной разработки и легитимную утилиту NirCmd. По нашим подсчетам, стоимость такого набора инструментов составляет не менее 66 000 долл. США.

В случае ПИР Банка денежные средства были выведены через карты физических лиц в 22 банках, причем большая часть похищенных средств обналичена в ночь проведения самой атаки. Для вывода и обналичивания денег киберпреступники обычно прибегают к услугам лиц, предоставляющих соответствующие схемы. Общая стоимость таких услуг, включая вознаграждение всем участникам преступной схемы

по снятию денег, составляет от 15% до 50% от суммы похищенных средств, а значит, группировке пришлось заплатить от 140 до 465 тыс. долларов за обналичивание украденных денег.

<p>Обналичивание средств сомнительного происхождения для ЮРИДИЧЕСКИХ ЛИЦ (ООО, ИП).</p> <p>от 25% - оперативная обработка и выплата средств.</p> <p>Индивидуальные условия для каждого клиента!</p> <p>Ваши средства будут там, где вы хотите их видеть.</p> <p>Подберу/изготовлю организации по Вашим требованиям.</p> <p>Обналичивание средств сомнительного происхождения для ФИЗИЧЕСКИХ ЛИЦ (КАРТЫ, КОШЕЛЬКИ)</p> <p>от 15% - выплата от 30 минут.</p> <p>Карты открыты в топовых банках.</p> <p>Оперативное снятие и последующая выплата средств.</p> <p>Идентифицированные, чистые кошельки к вашим услугам.</p> <p>О себе:</p> <p>Большой опыт работы. Наличие материала на любой вкус. Материал (ООО, Карты) на форуме не приобретаю. Толкаю блоки через арбитраж.</p>

Рисунок 18. Предложение нелегальных услуг по обналичиванию денег

Стоимость шпионской атаки оценить уже сложнее. Во-первых, за уязвимости нулевого дня на теневых форумах организаторы могут заплатить как десятки тысяч, так и миллионы долларов. Во-вторых, оценку усложняет использование самописного ПО, уникального для каждой группировки. История разработки такого ПО неизвестна, нет информации о том, сколько человек и в течение какого времени работали над его созданием, а следовательно, нет возможности оценить точную стоимость его разработки. Поэтому при подсчетах мы будем ориентироваться на минимальную стоимость заказной разработки ПО в дарквебе, чтобы получить представление о нижней границе цены.

Г АРТ38

41 000 000 \$

средний ущерб от успешной атаки

От 500 000 \$

стоимость одной атаки

В действиях еще одной финансово мотивированной группировки — АРТ38 — специалисты FireEye отмечают сходства с кибершпионскими кампаниями, в частности использование общих инструментов со шпионской группировкой TEMP.Hermit. На этапе проникновения группа применяет атаки типа watering hole, а среднее время присутствия в инфраструктуре жертвы составляет 155 дней, что в целом нехарактерно для атак, целью которых является кража денежных средств. Кроме того, в арсенале АРТ38 насчитывается 26 уникальных семейств вредоносного ПО, разработанных членами группировки. Примерная стоимость разработки такого набора инструментов, по нашей оценке, превышает 0,5 млн долларов.

В 2018 году эксперты PT ESC обнаружили АРТ-группировку TaskMasters, деятельность которой направлена главным образом на шпионаж в государственных организациях и промышленной сфере. Преступники имели доступ к различным важным сведениям: новым разработкам, договорам, финансовой отчетности и т. п. В подобных случаях ущерб для государства или отрасли промышленности колоссален, но его трудно измерить финансово. Примечательно, что в одной из компаний группировка оставалась незамеченной в инфраструктуре в течение 8 лет.

Г TaskMasters

От 300 000 \$

стоимость одной атаки после
проникновения в инфраструктуру

Вероятнее всего, для проникновения в инфраструктуру преступники используют схему supply chain attack. Находясь внутри сети, участники группировки применяют как бесплатные общедоступные утилиты, например из наборов NirSoft и Sysinternals Suite, так и собственные разработки: специалисты PT ESC выявили 15 оригинальных утилит, которые использовались в атаках. По приблизительным оценкам, стоимость разработки инструментов для проведения атаки внутри сети составляет не менее 300 тысяч долларов.

Г Выводы и рекомендации

Исследование показало, что инструменты, используемые хакерами при проведении АРТ, могут зависеть от мотивов киберпреступников. Оценочная стоимость арсенала инструментов финансово мотивированных группировок составляет несколько десятков тысяч долларов, для кибершпионских АРТ эта сумма на порядок больше. В то же время ущерб от АРТ для организаций-жертв в разы превышает затраты группировки на проведение атаки. Таким образом, затраты на приобретение или разработку инструментов для АРТ окупаются после первых успешных атак.

Мы рекомендуем финансовым организациям активно участвовать в обмене информацией о кибератаках и индикаторах компрометации, который постоянно происходит в отрасли. Центры мониторинга и реагирования на инциденты (например, ФинЦЕРТ Банка России) помогают значительно снизить успешность кибератак на кредитно-финансовую сферу. Кроме того, необходимо быть готовым оперативно выявлять следы атак в своей инфраструктуре. Крайне важно постоянно отслеживать аномальную активность в сети своей компании, чтобы обнаруживать и исследовать новые неизвестные атаки, делиться такой информацией с другими финансовыми организациями.

Характерной чертой шпионских кампаний сегодня является использование ПО собственной разработки и эксплойтов для уязвимостей нулевого дня. Такие группировки готовы уделять значительное время разведке и подготовке уникальных инструментов для обхода конкретных систем защиты, ведь они атакуют конкретную цель, и любая ошибка может привести к провалу всей операции. Поэтому обнаружить атаку кибершпионов в момент проникновения в локальную сеть сегодня невозможно, крайне сложно сделать это и на этапе закрепления и распространения в инфраструктуре. Зачастую ситуация усугубляется неготовностью самой инфраструктуры атакованной организации к выявлению атак.

Надеяться на защиту отдельных серверов и рабочих станций с помощью типовых решений бесполезно. Сегодня важно понимать, насколько эффективны те системы, которые внедрены в компании для обеспечения безопасности ключевых активов. Преступники уже давно научились обходить антивирусы, «песочницы», системы обнаружения вторжений. Компаниям необходимо реализовать комплексный подход, позволяющий не только сузить круг возможностей нарушителя, но и обеспечить максимальное понимание происходящих в инфраструктуре событий безопасности в контексте системных журналов, трафика и объектов, циркулирующих в сети. Только при полном понимании происходящих в инфраструктуре событий возможно построение процесса threat hunting, который позволяет успешно выявлять действия АРТ-группировок уже внутри инфраструктуры.

Глубокий анализ трафика, ретроспективный анализ событий ИБ, профилирование действий пользователей и возможность исследования оперативной памяти, процессов и других форензик-артефактов позволяют значительно сократить

время присутствия злоумышленников в инфраструктуре и предотвратить достижение поставленных ими целей. И конечно, средства защиты будут неэффективны против АРТ без поддержки высококвалифицированных специалистов в области расследования инцидентов.

Только понимание современных техник и тактик атакующих, знание используемых ими инструментов и готовность к выявлению наиболее часто применяемых методов атак с учетом специфики отрасли, целей и мотивов потенциального нарушителя позволят построить действительно эффективную защиту, обнаружить присутствие злоумышленника до того, как он достигнет своей цели, устранить угрозу и тем самым минимизировать ключевые риски компании.

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.