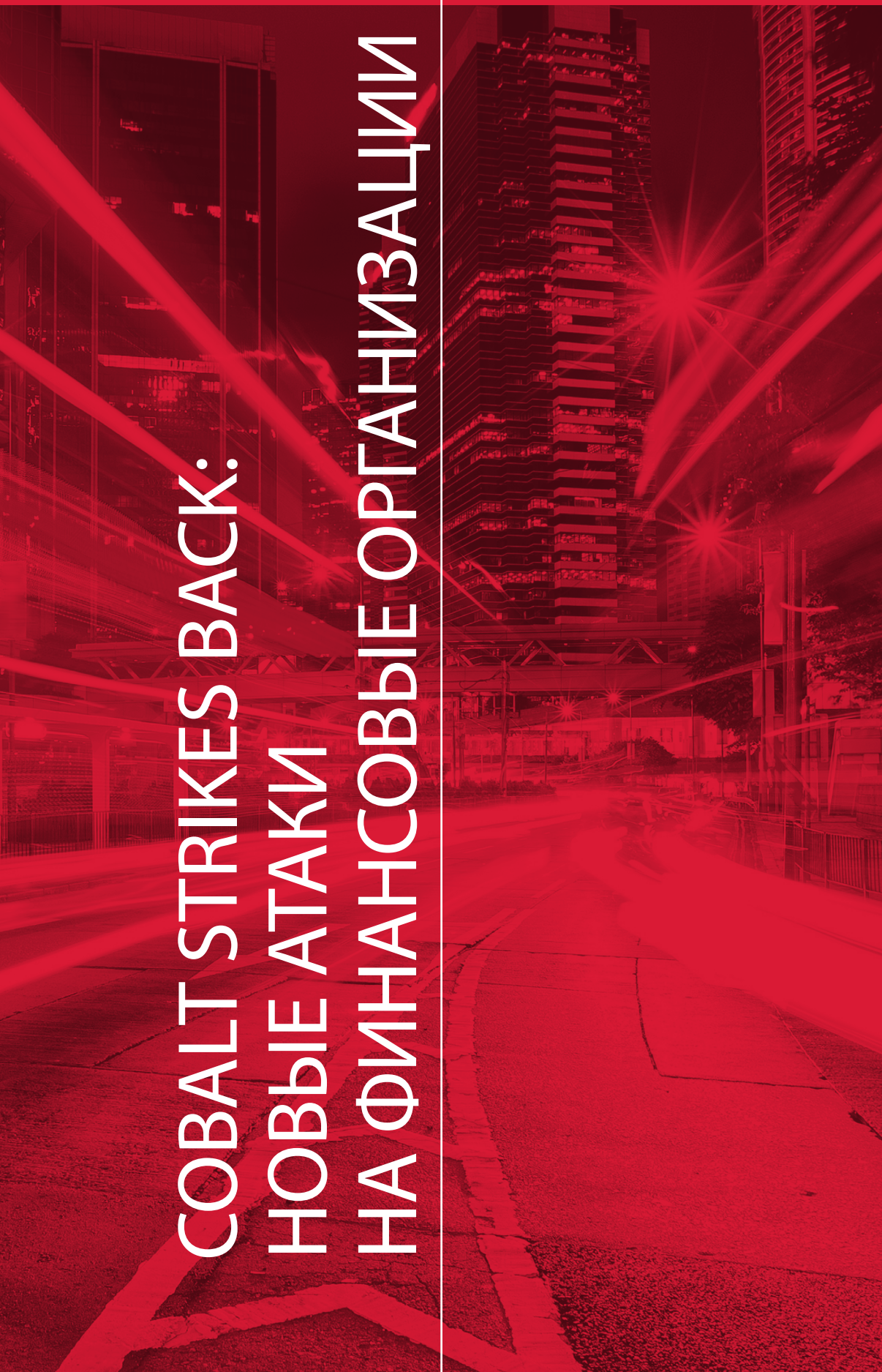


COBALT STRIKES BACK: НОВЫЕ АТАКИ НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

POSITIVE TECHNOLOGIES



СОДЕРЖАНИЕ

Введение.....	3
1. Резюме.....	3
2. Что мы знали о Cobalt раньше.....	4
3. Цели группы Cobalt сегодня	5
4. Хронология кампании Cobalt 2017	6
5. Методология атак группы Cobalt.....	8
5.1. Фишинговая рассылка через контрагента.....	9
5.2. Вредоносные вложения	13
5.3. Особенности инфраструктуры группы Cobalt.....	17
Заключение.....	19

ВВЕДЕНИЕ

Ограбление банка — классический пример остросюжетной истории, актуальный на протяжении многих веков. Куш, который можно сорвать, выбрав в качестве цели атаки именно банк, всегда прельщал злоумышленников. С течением времени изменилось многое — методы атак, типичный портрет грабителя, технические средства, размеры хищений. Не меняются лишь цель (деньги) и устоявшееся правило — «абсолютно защищенной системы не существует».

Сегодня, в эпоху цифровых экономик, это наиболее актуально: злоумышленники находят все новые методы мошенничества и атак, которые позволяют им похищать миллиарды, не выходя из дома. Несмотря на все механизмы защиты, которые применяются банками, уязвимости систем и человеческий фактор по-прежнему не позволяют полностью гарантировать безопасность. К сожалению, лишь малая часть организаций готова сегодня противостоять целевой атаке, что подтверждается на примере кампаний действующей сегодня по всему миру группировки Cobalt. Эта преступная группа специализируется на целенаправленных кибератаках на финансовые организации с целью кражи денег и известна с 2016 года.

Ранее мы и многие другие исследователи¹ уже приводили описание методов, которые использует эта группа. В этом отчете мы расскажем о новых техниках, которые Cobalt применяет в 2017 году, и дадим рекомендации, как не стать ее жертвой. Сегодня под их прицел попали не только банки.

1. РЕЗЮМЕ

Сегодня мы наблюдаем, как группа Cobalt быстро реагирует на вводимые банками меры защиты. Когда большая часть фишинговых писем с подделанным отправителем начала блокироваться спам-фильтрами на почтовых серверах, злоумышленники изменили технику. Теперь они активно атакуют поставщиков и контрагентов банков (Supply Chain Attack²), для того чтобы использовать их инфраструктуру и учетные записи реальных сотрудников для развития атак на другие организации. Подобная тактика уже использовалась другими злоумышленниками, например когда через инфраструктуру компании M.E.Doc нарушители распространили вирус NotPetya, который заблокировал рабочие станции во многих крупных организациях³.

Сегодня Cobalt атакует не только банки, но и биржи, страховые компании, инвестиционные фонды и другие напрямую связанные с финансами организации. Группа не боится использовать имена регуляторов и тематику информационной безопасности для отправки фишинговых писем с поддельных доменов.



В этом году группа Cobalt:

- + **Активно атакует контрагентов** для последующей рассылки фишинговых писем банкам через скомпрометированную инфраструктуру.
- + **Проводит фишинговые рассылки от имени финансовых регуляторов.**
- + **Использует вредоносные вложения различных типов:** документ с эксплойтом (.doc, .xls, .rtf), архив с исполняемым файлом дроппера (.scr, .exe), архив с LNK-файлом (.lnk).
- + **В числе первых получила доступ к последней версии эксплойт-билдера Microsoft Word Intruder 8**, чтобы создавать документы, эксплуатирующие уязвимость CVE-2017-0199.
- + **Использует публичные сайты со слабой защитой для загрузки на них вредоносных файлов** с целью их последующей доставки на целевые компьютеры.
- + **Осуществляет рассылки не только на корпоративные почтовые адреса, но и на личные адреса сотрудников.**

¹ www.group-ib.ru/cobalt.html

² www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

³ www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

2. ЧТО МЫ ЗНАЛИ О COBALT РАНЬШЕ



Цель преступников

Кража денег



Основной фокус

Банки СНГ и Восточной Европы



Методы

Кибератаки на корпоративную информационную инфраструктуру банков.

Фишинговые письма для проникновения в локальную сеть



Техническое обеспечение

ПО Cobalt Strike, средство удаленного администрирования Ammyy Admin, сканер SoftPerfect Network Scanner, утилита Mimikatz, встроенные функции ОС (PowerShell, PsExec, Runas)

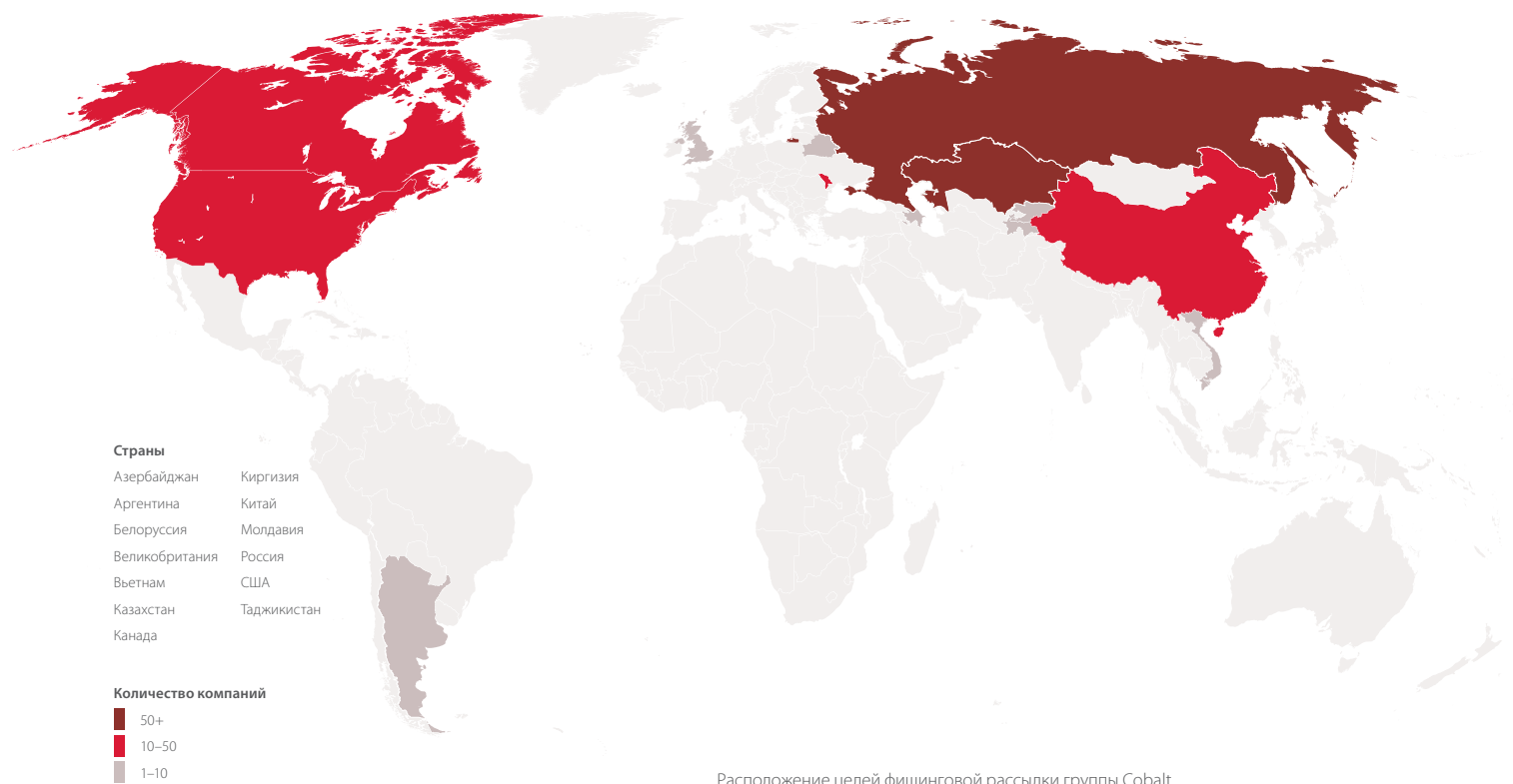


Типовая схема атаки

1. Целевая рассылка фишинговых писем сотрудникам банка.
2. Заражение компьютера сотрудника, открывшего вложение.
3. Распространение атаки внутри сети банка, компрометация узлов, связанных с управлением банкоматами.
4. Заражение банкоматов вредоносным ПО для манипуляций с диспенсером.
5. Выдача денег, которые забирают подставные лица — дропы, или money mules.

3. ЦЕЛИ ГРУППЫ COBALT СЕГОДНЯ

В 2017 году к списку обычных для группы Cobalt целей, находящихся в странах СНГ, Восточной Европы и Юго-Восточной Азии, добавились компании, расположенные в Северной Америке, Западной Европе и даже в Южной Америке (в Аргентине).



Деятельность около 75% компаний, включенных группой в список для рассылки фишинговых писем, связана с финансами. Несмотря на то что большую часть из них составляют банки (90% атакованных финансовых организаций), в их число также входят фондовые биржи, инвестиционные фонды и другие специализированные кредитно-финансовые организации. Расширение целей группы Cobalt по сферам деятельности свидетельствует о готовящихся атаках на другие организации, так или иначе связанные с крупным оборотом денежных средств. Это подтверждает прогноз FinCERT Центрального банка России о повышении интереса киберпреступников в 2017 году именно к биржам⁴.

При успешной атаке на фондовую биржу злоумышленники своими действиями могут спровоцировать участников на покупку или продажу акций определенных компаний, что приведет к изменению котировок их акций на большое количество пунктов за короткий промежуток времени и повлечет за собой серьезные последствия, которые могут сказаться не только на прибыли компаний, но и на экономике страны. Подобные методы использовала группа Corkow в атаках на Энергобанк в 2016 году; тогда действия злоумышленников привели к изменению курса рубля более чем на 15% и повлекли финансовые потери организации в размере 244 млн рублей⁵.

С начала 2017 года мы проанализировали более 60 уникальных образцов писем, относящихся к кампаниям группы Cobalt. Их адресатами стали более 3 тыс. получателей, находящихся в 13 странах. В списке получателей присутствуют не только корпоративные почтовые адреса, но и личные адреса сотрудников, поскольку те могут проверять личную почту на рабочем месте.

Отметим, что злоумышленники также атакуют государственные учреждения с целью использования их в качестве промежуточного звена в цепочке атак.

В оставшиеся 25% входят компании из следующих сфер деятельности:

- + госучреждения;
- + телеком и интернет;
- + сфера услуг;
- + промышленность;
- + сфера развлечений;
- + медицина.

4 www.rbc.ru/finances/02/02/2017/589353b09a794757b187f14f

5 www.rbc.ru/finances/08/02/2016/56b89bab9a7947474f91de83

Май

9. Получение обновления MVI 8 с возможностью создавать документы, нацеленные на уязвимость CVE-2017-0199
10. Регистрация новых фишинговых доменов и настройка DNS-серверов
11. Фишинговые рассылки с новыми документами (CVE-2017-0199)
12. Повторные попытки атак на контрагентов, которые были отражены

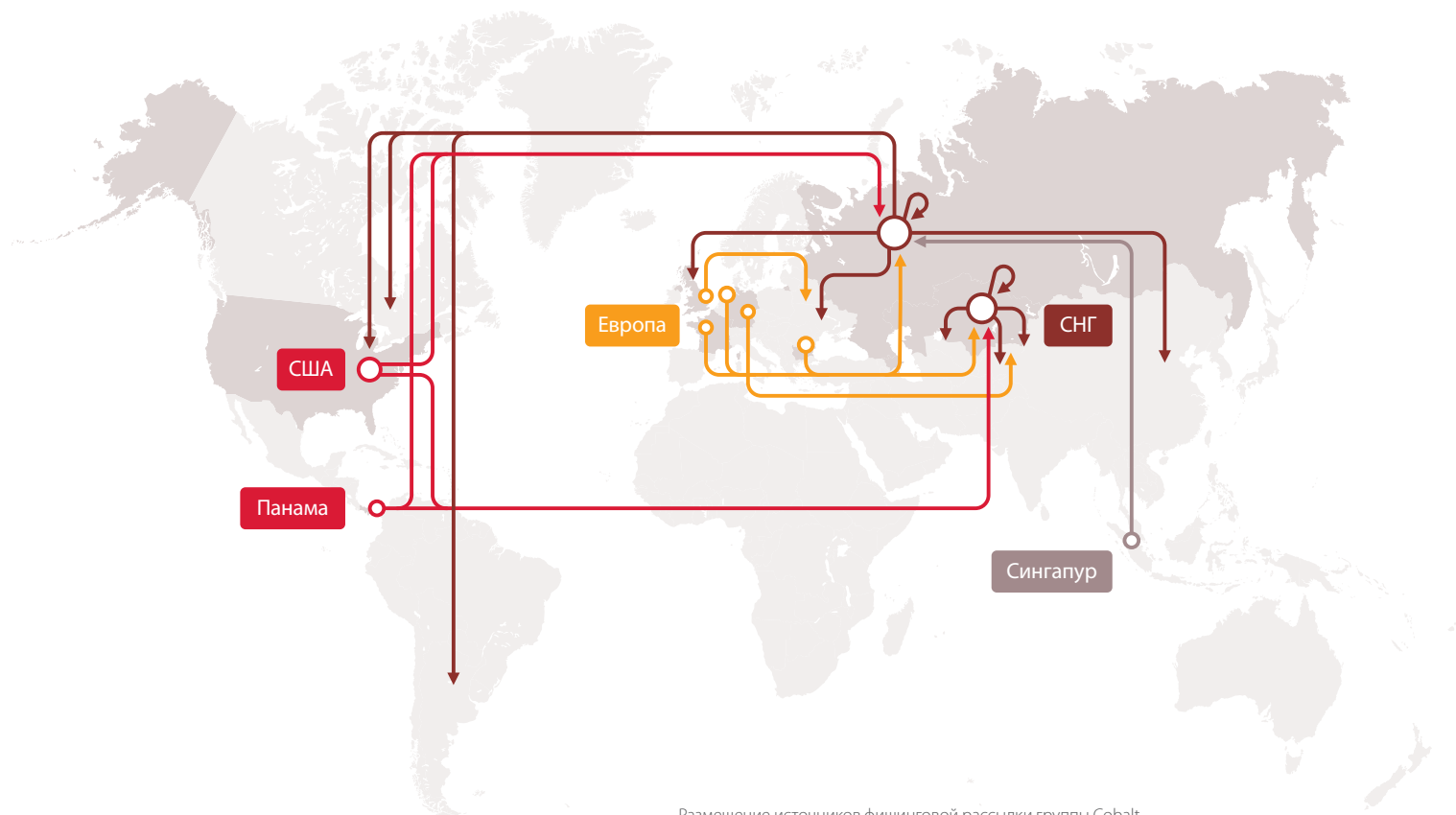


В начале 2017 года мы зафиксировали, что группа Cobalt активно регистрирует поддельные домены. При выявлении рассылок с этих доменов мы уведомляли подразделения ИБ организаций, которые значились в списке получателей писем, а также FinCERT Центрального банка России. Наши действия позволили блокировать домены до того, как злоумышленники ими воспользовались.

В 2017 году компания Positive Technologies проводила расследования инцидентов, связанных с атаками группировки Cobalt, в ряде компаний. Было выявлено, что сразу в нескольких из них злоумышленники использовали инфраструктуру и учетные записи сотрудников для рассылки фишинговых писем в адрес других компаний-контрагентов, расположенных в странах Северной и Южной Америки, Европы, СНГ, Центральной и Юго-Восточной Азии. Для компрометации компаний в странах СНГ помимо этого использовались и узлы собственной инфраструктуры злоумышленников, в том числе арендованные выделенные серверы, расположенные в Северной Америке, Европе, Юго-Восточной Азии.

Принятые в ходе реагирования на инциденты меры позволили не только выявить и остановить деятельность нарушителей в рамках сетевой инфраструктуры контрагентов, но и предотвратить повторную компрометацию, которую злоумышленники пытались осуществить после потери контроля. Компании, в адрес которых осуществлялись рассылки от имени сотрудников контрагентов, были оповещены об опасности компрометации.

Атаками на различные организации по всему миру злоумышленники не ограничились — это был лишь промежуточный этап. В случае успешной атаки на банк или другого контрагента злоумышленники проводили дальнейшую рассылку и развивали атаку на другие банки.



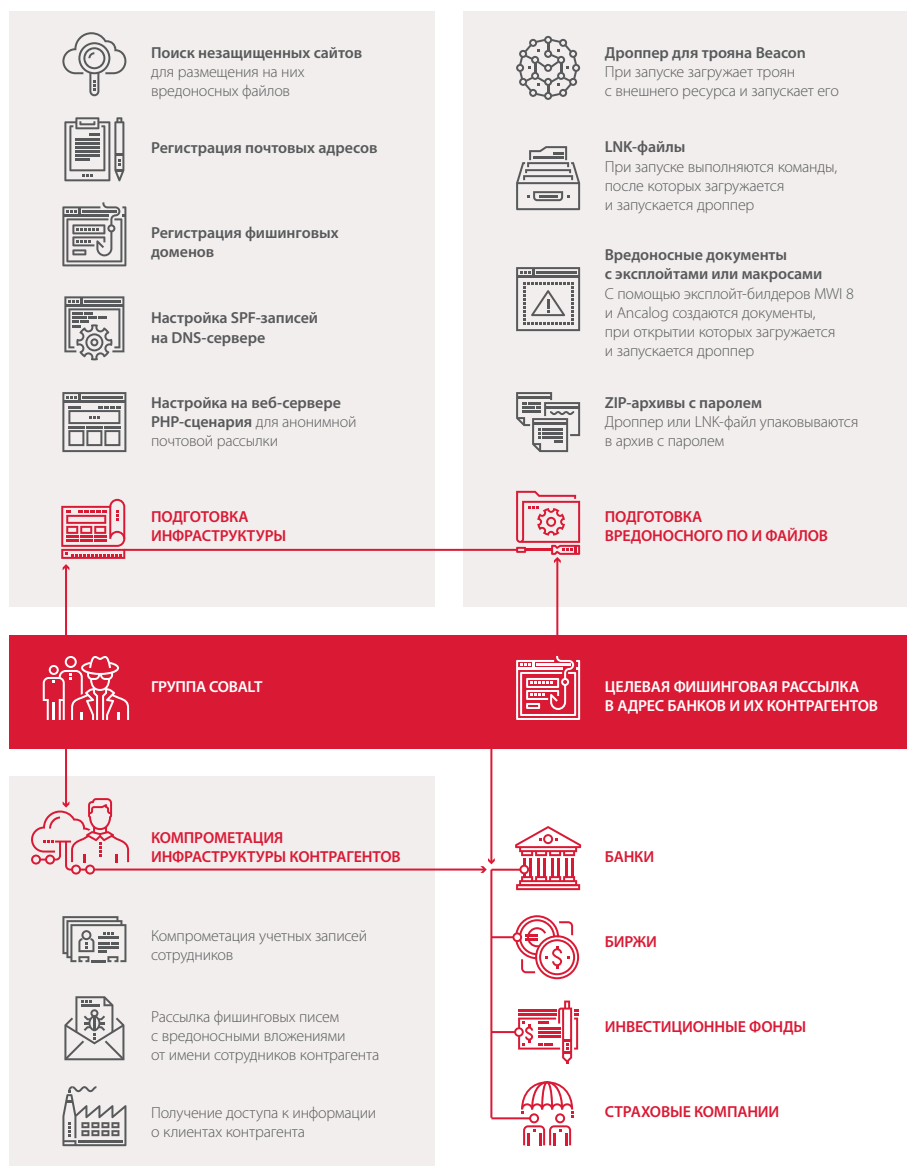
Размещение источников фишинговой рассылки группы Cobalt

Было замечено, что на время активных действий внутри сети атакованных организаций группа переставала регистрировать новые доменные имена и проводить с них рассылку, также не было выявлено иной активности, не относящейся к компрометации атакованной инфраструктуры. Это может быть свидетельством того, что часть группировки, отвечающая за техническую составляющую атак, немногочисленна. Выявлены и другие факты, позволяющие сделать такой вывод, например время и дни осуществления рассылок (информация об этом приведена далее).

5. МЕТОДОЛОГИЯ АТАК ГРУППЫ COBALT

Группа Cobalt при проведении целевых атак проникает в сеть организации с помощью методов социальной инженерии, то есть пользователи сами загружают вредоносные вложения из фишинговых писем, которые злоумышленники рассылают от имени известных компаний и регулирующих организаций. Такие вложения содержат файл документа, загружающего дроппер с удаленного сервера, или сам дроппер в архиве с паролем. Дроппер — это небольшая вредоносная программа, предназначенная для загрузки и запуска другого вредоносного ПО (в случае Cobalt это троян Beacon).

Элементы этапа подготовки к целевой атаке и ее типовая схема приведены ниже.



Действия злоумышленников внутри сети атакованной организации подробно описаны в нашем прошлом отчете.⁶

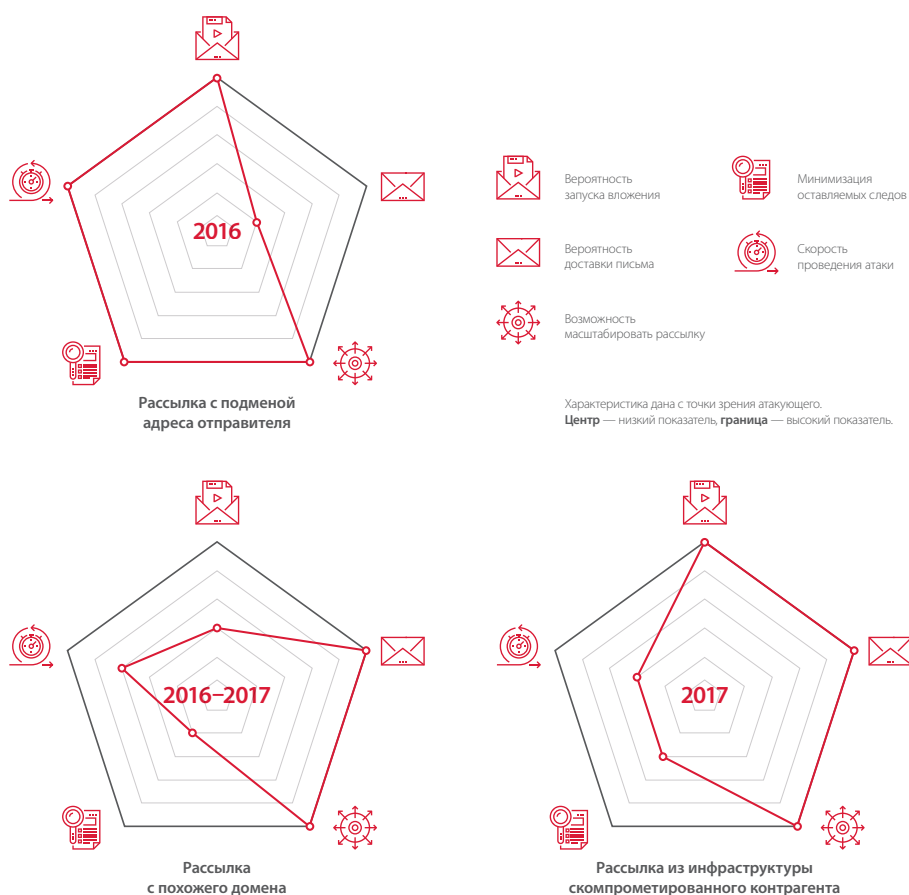
⁶ www.ptsecurity.com/upload/ptru/analytics/Cobalt-Snatch-rus.pdf

5.1. Фишинговая рассылка через контрагента

Ранее применявшийся группой Cobalt метод отправки писем с подменой адреса отправителя стал встречаться все реже, потому что злоумышленники стали уделять больше внимания доставке писем и прохождению ими фильтров на почтовом сервере.

Для целевой рассылки преступники используют предварительно зарегистрированные домены. Доменное имя подбирается схожим по смыслу и написанию с именем домена той компании, сотрудником которой злоумышленники хотят представиться. Чтобы письма проходили проверки антифишинговых и антиспам-систем, злоумышленники корректно настраивают SPF-записи на DNS-сервере и указывают корректные DKIM-подписи для создаваемых писем. Этот подход позволяет обойти верификацию адреса почтового сервера отправителя, но оставляет дополнительные цифровые следы для криминалистов.

Несмотря на более высокую сложность реализации атаки, в первом квартале 2017 года группа Cobalt также стала атаковать различные компании, сотрудничающие с банками, а затем активно рассылать фишинговые письма непосредственно из инфраструктур этих организаций с использованием учетных записей и почтовых адресов их сотрудников.



Этот подход по сравнению с другими перечисленными методами обладает рядом преимуществ:

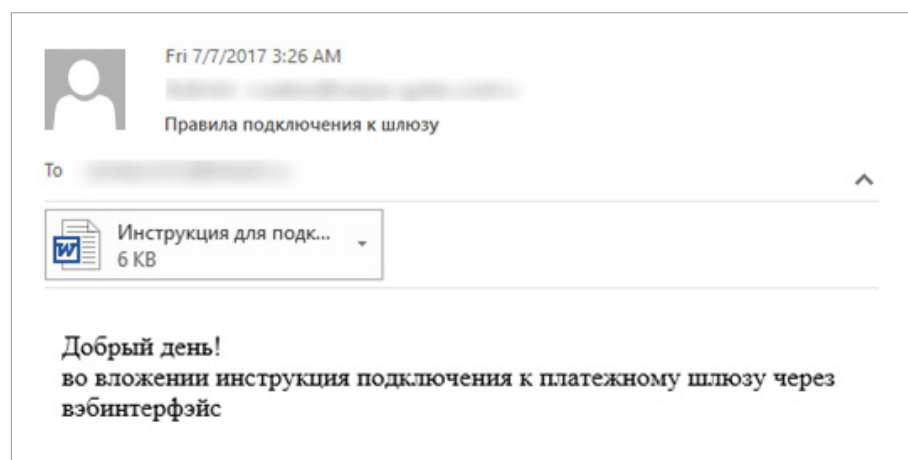
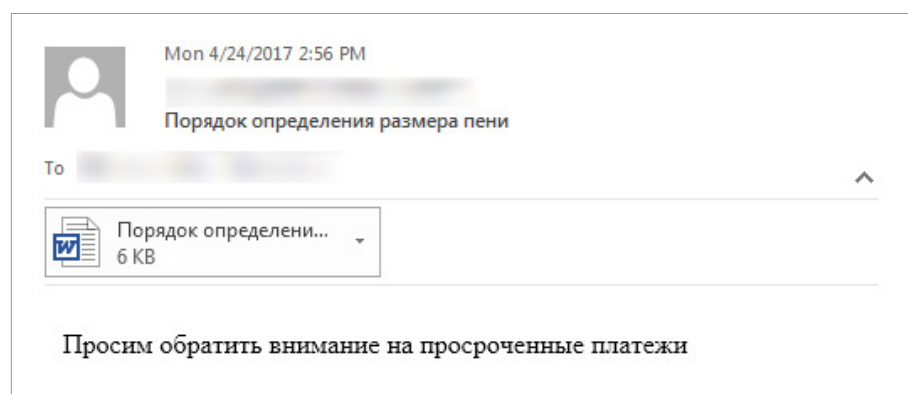
- + Позволяет получить доступ к информации, находящейся на серверах и в базах данных скомпрометированной организации, которая может быть использована при составлении фишинговых писем.
- + Позволяет получить доступ к учетным записям сотрудников на рабочих станциях и почтовом сервере, что обеспечивает фишинговым письмам высокий уровень доверия получателей и правдоподобную легенду.
- + Письма от партнеров и контрагентов не блокируются системами фильтрации, установленными на почтовых серверах.



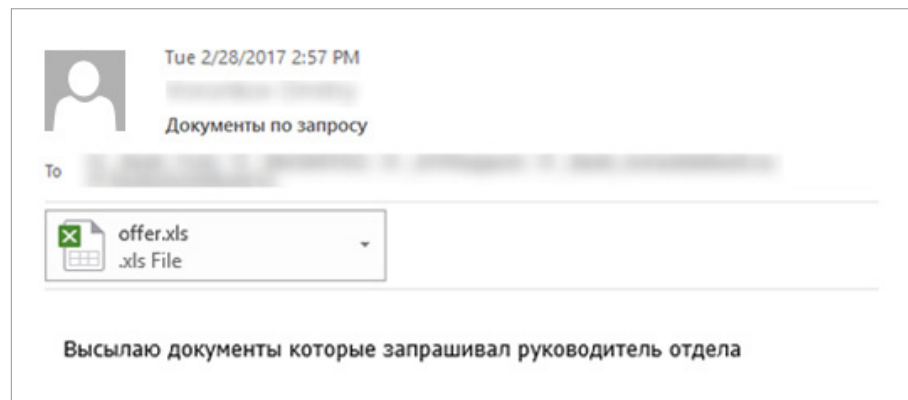
При фишинговой рассылке злоумышленники создают письма с такими темами, адресами отправителей, содержанием, названиями вложений, чтобы не вызывать подозрения у получателей и тем самым побудить их к запуску вредоносных вложений.

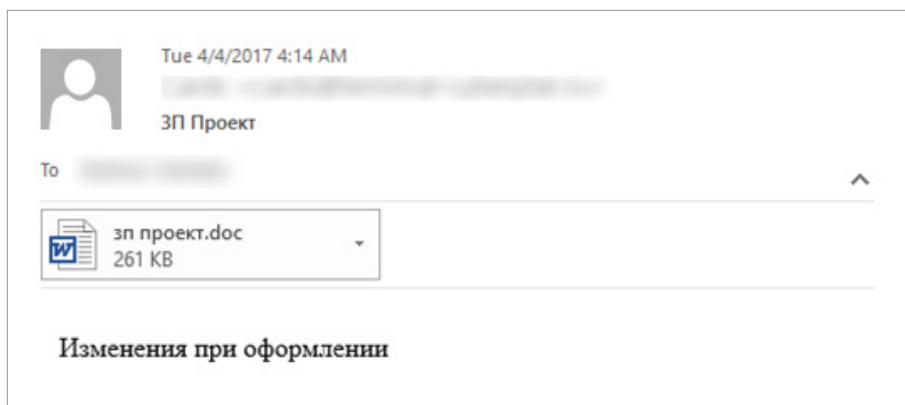
Сегодня группа Cobalt использует фишинговую рассылку практически на всех этапах целевых атак на банки.

1. Первичная компрометация одной или нескольких рабочих станций организации контрагента с помощью фишинговой рассылки.

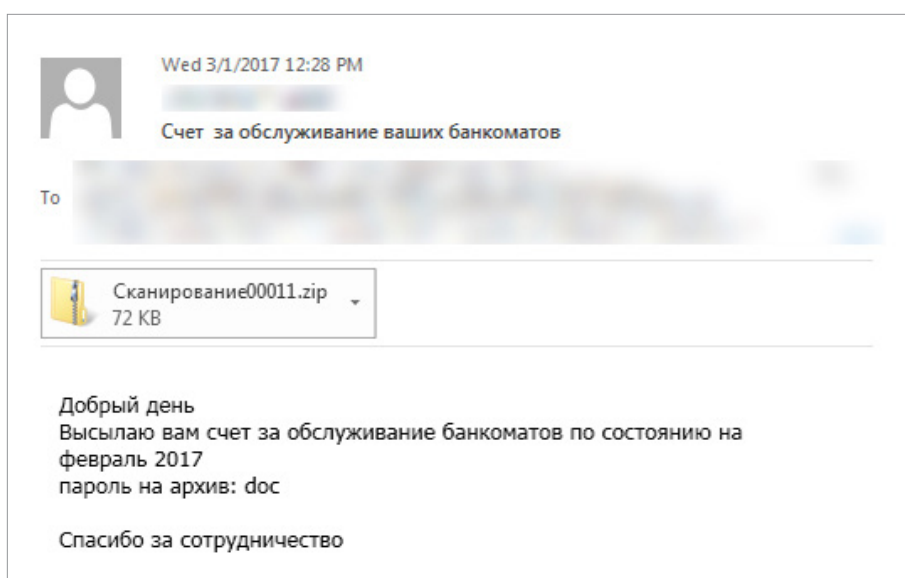


2. Развитие атаки в сети организации с помощью внутренней рассылки писем с вредоносными документами от имени коллег, руководства или сотрудников IT-отделов.

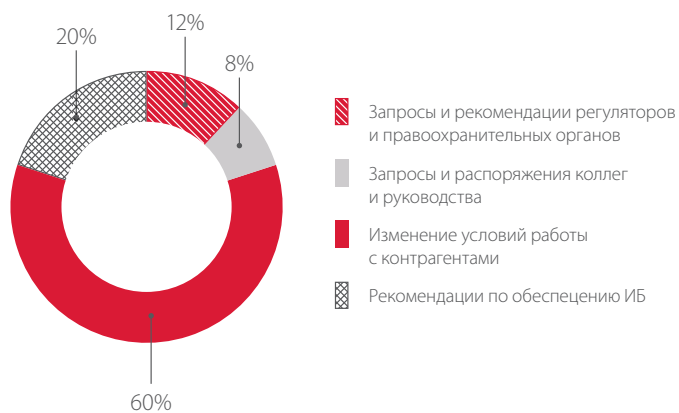




3. Рассылка вредоносных писем из инфраструктуры контрагента в адрес банков и других организаций, напрямую связанных с финансами.

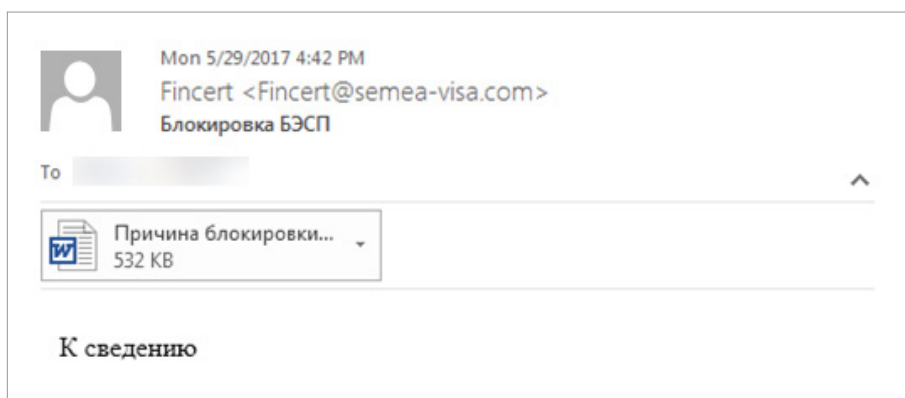
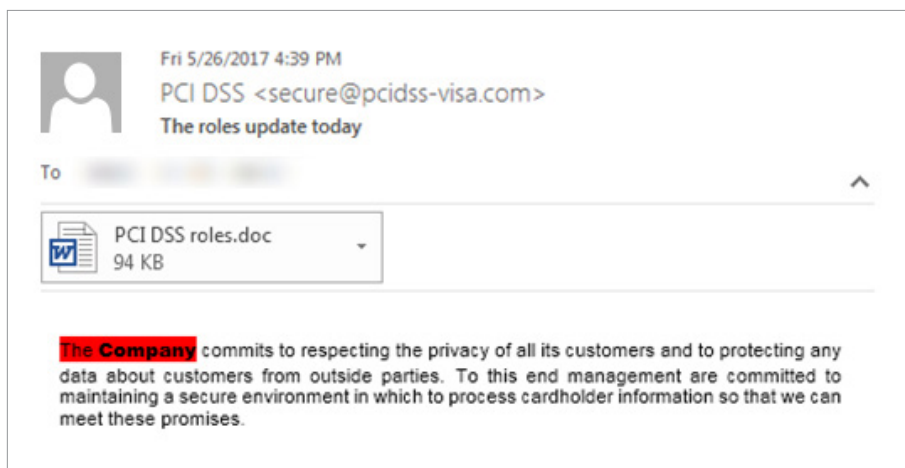


В начале 2017 года 60% фишинговых писем от группы Cobalt были связаны с тематикой условий сотрудничества и порядка оказания услуг между банками и их контрагентами.

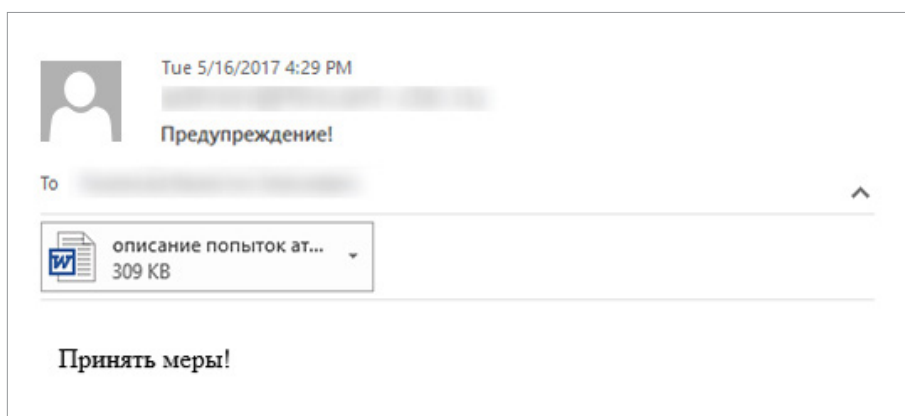


Тематика фишинговых писем

В 2017 году Cobalt стала еще активнее использовать тему информационной безопасности. Подобные письма злоумышленники рассылали с поддельных доменов, в том числе от лица платежных систем Visa и MasterCard, FinCERT Центрального банка России и Национального Банка Республики Казахстан.

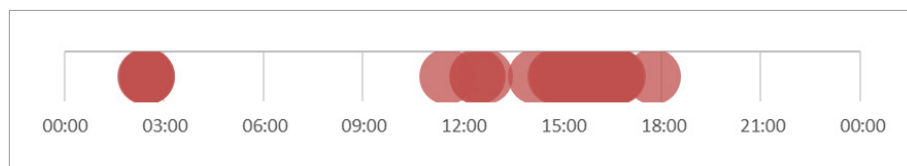


На территории России это связано с тем, что FinCERT начал активно предупреждать кредитно-финансовые организации об активности данной группы. Злоумышленники воспользовались этим и стали рассылать банкам письма с вредоносными документами, якобы содержащими инструкции по информационной безопасности.

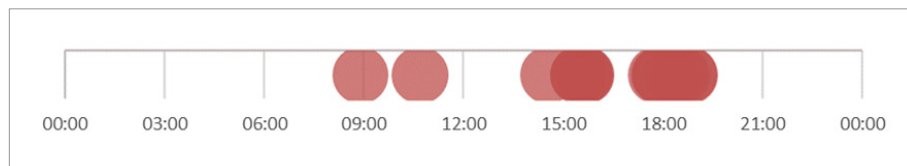


Таким образом, создавая поддельные домены, схожие по написанию с доменами реальных компаний, злоумышленники используют авторитет и полномочия этих организаций, чтобы убедить пользователей открыть вложение.

Так как письма от коллег, контрагентов и партнеров обычно приходят в рабочее время, для большей достоверности злоумышленники проводили рассылку таким образом, чтобы письма доставлялись в рабочее время получателей (независимо от того, из какого часового пояса они действовали).



Время получения писем компаниями из Восточной Европы (UTC+3)



Время получения писем компаниями из Центральной и Южной Азии (UTC+6)

Время получения большей части писем приходится на вторую половину рабочего дня. Выбор такого времени обусловлен тем, что бдительность сотрудников к вечеру заметно снижается, и это повышает шансы на компрометацию рабочей станции.

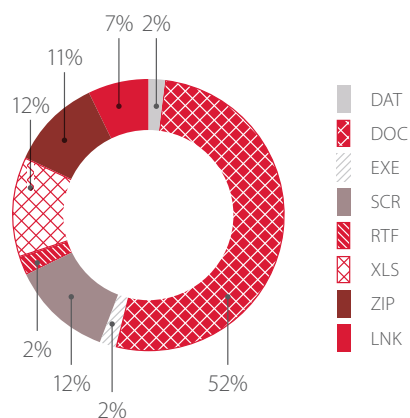


Время получения писем компаниями из Северной Америки (UTC-4)

Иную тактику мы заметили в случае отправки писем в североамериканские компании. Письма в адрес организаций из США и Канады рассылались через скомпрометированную инфраструктуру контрагента, находящегося в Европе. Для того чтобы активность злоумышленников была замаскирована под обычную деятельность сотрудников, рассылка проводилась в рабочие часы этой компании, поэтому доставка писем в Северную Америку приходилась на раннее утро.

5.2. Вредоносные вложения

Для организации удаленного доступа к рабочему компьютеру сотрудника целевой организации группа Cobalt, как и раньше, использует троян Beason из состава коммерческого ПО для проведения тестов на проникновение Cobalt Strike.



Типы вредоносных файлов

Доставка и запуск трояна обеспечиваются с помощью специального загрузчика, который, в свою очередь, в виде SCR- или EXE-файлов попадает на компьютер жертвы разными способами:

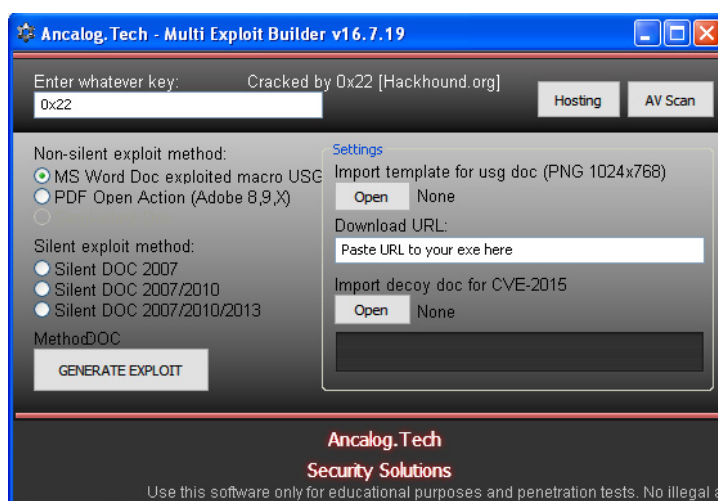
- + в ZIP-архиве с паролем, который сообщается жертве в тексте письма;
- + загружается с уязвимого сайта при запуске вредоносного документа (.doc, .xls, .rtf) из фишингового письма;
- + загружается с уязвимого сайта в ходе выполнения команд, прописанных в LNK-файле из ZIP-архива, приложенного к письму.

Из исследованных нами фишинговых писем, которые рассылала группа Cobalt, 52% содержали документы Microsoft Word.



Сайты со слабой защитой компрометируются злоумышленниками и используются ими как файловые хостинги для размещения вредоносных файлов, применяемых в целевых атаках на банки.

Вредоносные документы Microsoft Office, которые злоумышленники используют для загрузки дроппера, создаются с помощью эксплойт-китов Ancalog и Microsoft Word Intruder (MWI). Это программное обеспечение позволяет пользователю, не обладающему навыками программирования, за несколько минут создавать вредоносные документы и PDF-файлы в интуитивно понятном интерфейсе.



Группа Cobalt в числе первых получила доступ к ограниченной версии MWI, которая позволяет создавать документы, эксплуатирующие критически опасную уязвимость CVE-2017-0199. Учитывая то, что данная версия продавалась поштучно и только тем, с кем у автора MWI сложились доверительные отношения, мы не исключаем связи между злоумышленниками и разработчиком эксплойт-билдера. Это подтверждается и тем, что между первыми фишинговыми рассылками группы, в которых использовались документы с эксплойтами для уязвимости CVE-2017-0199, и публикацией объявления о выходе новой версии MWI прошло меньше недели⁷.

[+] MWISTAT 2.0
MICROSOFT WORD INTRUDER

FILES | LOGS | STATS | TOOLS

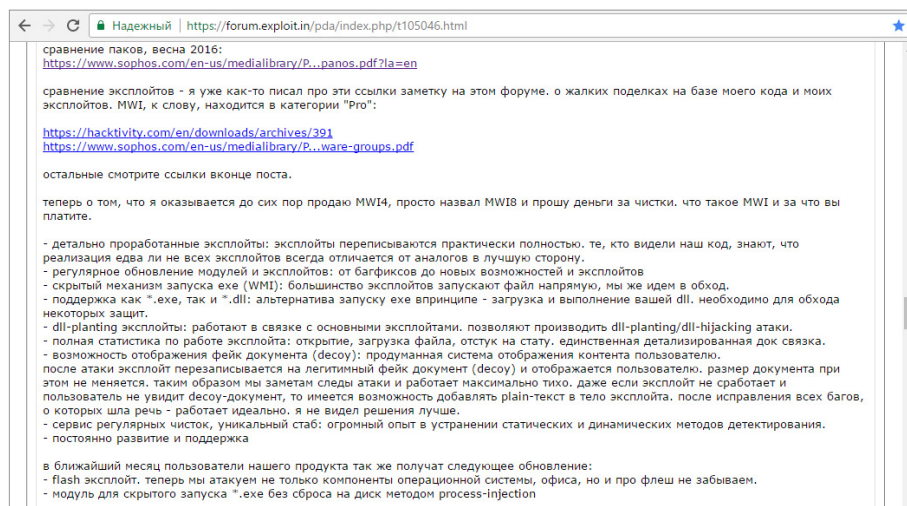
NAVIGATION: FILES

FILE ID	FILE NAME	FILE SIZE	FILE DATE	FILE STAT URL	FILE LOGS	ACTION
00000000	-	-	-	-	LOGS STATS	-
12123434	putty.exe	472 kb	December 10 2014 00:19:46	stat:http://localhost/mwistat/image.php?id=12123434	LOGS STATS	GET EDIT DEL
12341234	msgbox.exe	1 kb	December 08 2014 15:15:23	stat:http://localhost/mwistat/image.php?id=12341234	LOGS STATS	GET EDIT DEL

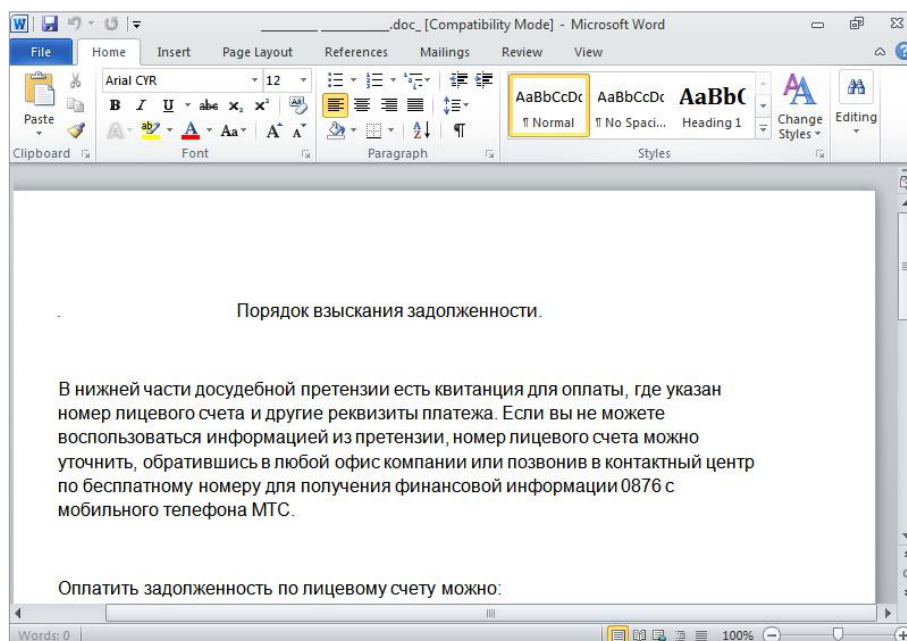
ADD NEW FILE

⁷ www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target

Также отметим, что MWI позиционируется разработчиком как инструмент создания документов для проведения APT, а за использование созданных с помощью эксплойт-билдера файлов в спам-рассылках автор отзывает лицензию. Пользователям ограниченной версии MWI предлагается услуга «очистки», в результате которой вредоносные файлы на момент их создания не распознаются известными антивирусными системами.



Вредоносные документы, которые группа Cobalt рассылает банкам и их контрагентам, используют эксплойты для уязвимостей CVE-2017-0199, CVE-2015-1641, CVE-2012-0158, чтобы загружать и запускать дроппер на атакуемой системе.



При открытии вредоносного документа выполняется вредоносный код, который, эксплуатируя уязвимости в Microsoft Office, обеспечивает загрузку дроппера с удаленного сервера и его запуск⁸. После того как вредоносный код отработал, жертве показывается заранее подготовленный злоумышленниками документ (decoy, см. снимок экрана выше).

⁸ blog.fortinet.com/2017/05/30/spear-phishing-fileless-attack-with-cve-2017-0199



Загрузка вредоносного ПО на предварительно взломанный сайт

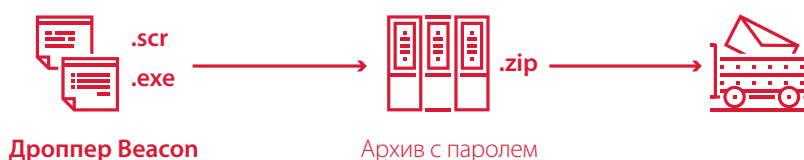
Злоумышленники размещают вредоносные файлы на уязвимых сайтах, чтобы впоследствии их можно было загрузить из инфраструктуры жертвы во время атаки. Поэтому мы настоятельно рекомендуем владельцам сайтов внимательно следить за защитой своих ресурсов: существует вероятность стать звеном в цепочке целевой атаки, что приведет к блокировке сайта регулятором или изъятию серверного оборудования правоохранительными органами в ходе расследования совершенного преступления, а огласка подобного инцидента нанесет существенный удар по репутации компании.

Обычно злоумышленники из Cobalt проводят рассылку вредоносных писем в несколько этапов. В первой волне рассылаются документы Microsoft Office, созданные в эксплойт-китах.



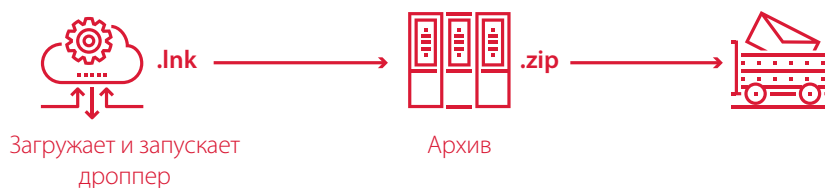
Первая волна рассылки писем с вредоносными вложениями

Если в течение суток после рассылки не было зафиксировано ни одного успешного запуска вредоносных файлов, например потому, что в компании установлены актуальные обновления Microsoft Office, в которых исправлены критически опасные уязвимости, на которые рассчитаны эксплойт-билдеры, используемые злоумышленниками, — то проводится вторая рассылка.



Вторая волна рассылки писем с вредоносными вложениями

Во второй волне группа Cobalt в качестве вложения использует дроппер в виде исполняемых файлов с расширениями .exe или .scr, размещенных в архиве с паролем. Это помогает обойти некоторые системы фильтрации и антивирусную защиту. На сегодняшний день существуют решения, позволяющие в режиме реального времени проверять содержимое приложенных архивов, если пароль указан в тексте письма, однако такие системы применяют далеко не все организации, что на руку злоумышленникам.

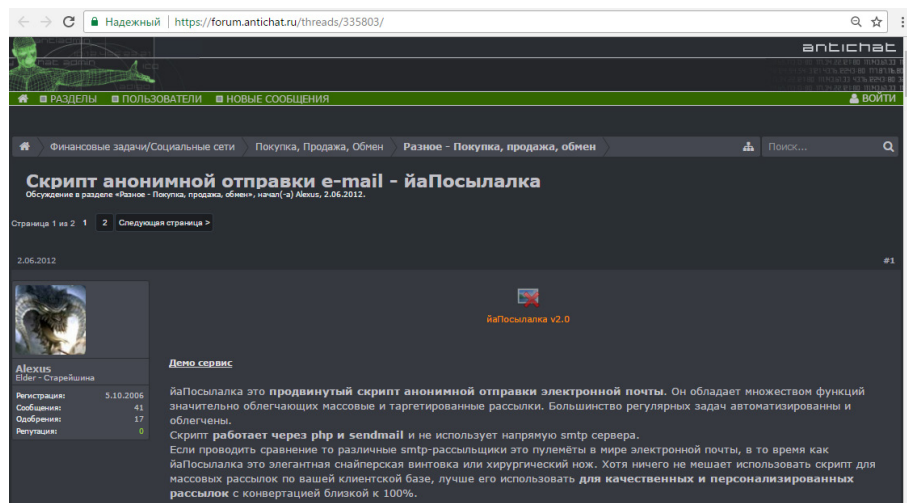


Рассылка писем с вредоносными вложениями

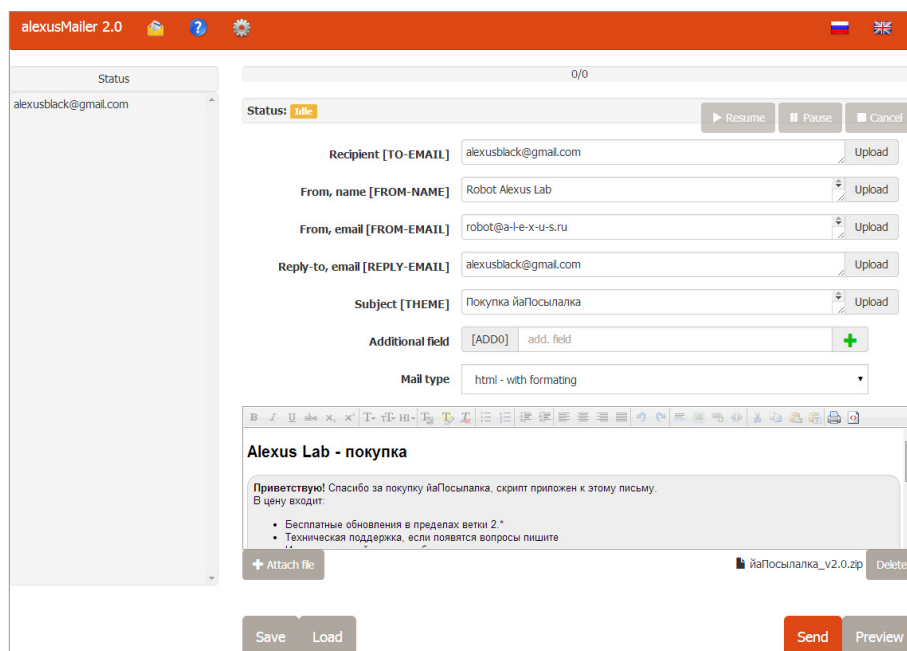
Кроме того, мы зафиксировали отдельную рассылку писем с вложенными архивами, содержащими LNK-файлы, также загружающими дроппер трояна Beacon.

5.3. Особенности инфраструктуры группы Cobalt

Поскольку список получателей фишинговой рассылки группы Cobalt насчитывает тысячи адресов, то очевидно, что злоумышленники используют средства автоматизации. В ходе анализа образцов писем установлено, что для отправки писем с фишинговых доменов используется свободно распространяемый PHP-сценарий анонимной отправки почтовых сообщений «ЙаПосылалка», который также известен как alexusMailer v2.0⁹.



Функциональность сценария включает поддержку многопоточной отправки, визуальный редактор письма, возможность загрузки получателей и всех основных полей из файлов, поддержку шаблонов, возможность прикрепления любого количества файлов к письму и другие опции. Пользователь может использовать множество серверов для распределения рассылки и устанавливать задержку между отправкой писем.



Однако когда письма рассылаются с помощью alexusMailer, в заголовке письма остается артефакт в виде поля X-PHP-Originating-Script, содержащего имя файла PHP-сценария, используемого для отправки писем. Это свидетельствует о том, что на серверах, с которых проводится рассылка, в конфигурационном файле php.ini установлены параметры журналирования рассылаемой почты.

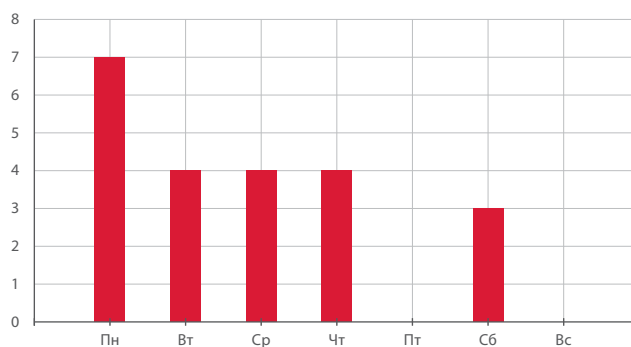
⁹ github.com/AlexusBlack

```
Received: from www-data by pcidss-visa.com with local (Exim 4.80)
(envelope-from <www-data@pcidss-visa.com>) id 1dEFNs-0004JT-EX for
Fri, 26 May 2017 13:34:28 +0000
To:
Subject: =?UTF-8?B?V6h1IHJvbGVzIHVwZGF0ZS80b2RheQ==?=
X-PHP-Originating-Script: 0:slexusMailer_v2.0.php
From: =?UTF-8?B?UENJERTUw==?= <secure@pcidss-visa.com>
MIME-Version: 1.0;
Content-Type: multipart/mixed; boundary="--mPzo4To603"
Reply-To: <secure@pcidss-visa.com>
Message-ID: <E1dEFNs-0004JT-EX@pcidss-visa.com>
Date: Fri, 26 May 2017 13:34:28 +0000
```

Преступники используют широко известные публичные почтовые сервисы, а также сервисы, позволяющие анонимно зарегистрировать временный электронный почтовый ящик. Так, в некоторых рассылках группы Cobalt обратные адреса принадлежали следующим сервисам: TempMail (@doanart.com, @rootfest.net), Mail.com (@mail.com), AT&T Mail (@att.net, @sbcglobal.net), Yahoo! (@ymail.com). На этих же сервисах были созданы почтовые ящики, использованные при регистрации доменов.

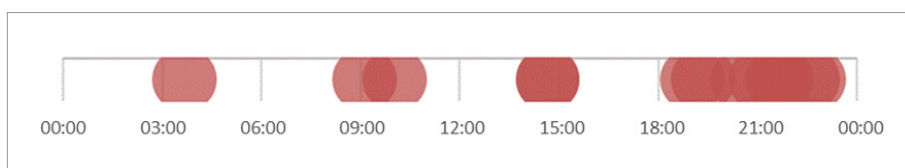
Проанализировав время регистрации доменов, входящих в инфраструктуру группы Cobalt, мы выявили, что злоумышленники активнее регистрировали домены в начале недели. Исходя из этого выдвинуты следующие предположения:

- + В рабочие дни злоумышленники активно регистрируют домены, подготавливают инструменты и в меньшей степени заняты рассылкой вредоносных писем.



Дни регистрации доменов

- + На конец недели приходится основная деятельность по рассылке писем и развитию атак внутри инфраструктуры скомпрометированных организаций.
- + В рабочие часы злоумышленники занимаются рассылкой фишинговых писем. Этим объясняется тот факт, что регистрация большей части доменов приходится на промежуток времени с 18:00 до 24:00 (в часовом поясе +0 по всемирному координированному времени, UTC+0) и проходит после окончания рабочего дня в европейских странах.



Время регистрации доменов (UTC+0)

Очевидно, что после регистрации домена в начале недели у группы Cobalt есть некоторое время для подготовки к запуску очередной кампании по рассылке фишинговых писем, которая, как было отмечено, производится в конце недели. Среднее время между регистрацией домена и первой фишинговой рассылкой с его использованием составляет четыре дня.

Наши эксперты выявили ряд фишинговых доменов нарушителей до того, как они были использованы для проведения рассылки, и использовали эту задержку, чтобы оперативно заблокировать эти домены.

На сегодняшний день в результате совместной работы с российскими и международными отраслевыми регуляторами все домены, выявленные в зоне .ru, и большая часть доменов в других зонах были сняты с делегирования.

ЗАКЛЮЧЕНИЕ

С каждым годом порог входа в киберпреступность снижается. Злоумышленникам теперь не надо искать уязвимости нулевого дня и приобретать дорогие инструменты для проведения атак — достаточно базовых навыков программирования и набора коммерческого ПО с инструкциями, размещенными в интернете.

Мы обращаем внимание банков и других компаний на то, что злоумышленники постоянно модифицируют и развивают свои инструменты и техники атак. Сегодня ваша организация может стать объектом атаки, даже не являясь конечной целью нарушителей, а будучи лишь звеном в цепочке атак. Поэтому нельзя оставаться в стороне от проблемы и считать, что опасности подвержены лишь крупные компании и финансовые учреждения или что атаки происходят где-то далеко, в другой части света. Каждой организации, будь то банк или государственное учреждение, необходимо поддерживать защиту инфраструктуры в актуальном состоянии, своевременно обновляя ПО и ОС. Необходимо проводить тренинги для сотрудников с целью повышения их осведомленности в вопросах информационной безопасности. Особенно важно не только тщательно следить за входящими письмами, включая вложенные файлы, но обращать внимание на исходящую почту и проводить ретроспективный анализ. Также необходимо следить за защитой внешних веб-приложений, ведь использование злоумышленниками инфраструктуры компании или ее веб-ресурсов в рамках атак может нанести серьезный ущерб репутации компании, а также повлечь блокировку ресурсов в случае попадания их адресов в списки индикаторов компрометации, а это часто означает уже не только репутационные, но и прямые финансовые потери.

На сегодняшний день мы не обладаем информацией о фактических убытках компаний от деятельности группы Cobalt в 2017 году. Возможно, действия регуляторов, предупреждающих банки об угрозе компрометации, существенно усложнили злоумышленникам задачу. Мы продолжаем наблюдать за активностью группы Cobalt и будем сообщать новые сведения по мере их появления. Исходя из масштабов, которых достигли кампании группировки Cobalt по всему миру, исключать многомиллионные потери банков нельзя, а в случае успешных атак на фондовые биржи возможны не только финансовые потери отдельных организаций, но и изменение курсов валют.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.