

ВУНТРАР

Эволюция целенаправленных
атак на банки

ОГЛАВЛЕНИЕ

Введение	2
Ключевые результаты	3
Начало: атаки на клиентов банков	5
Способы распространения	9
Атаки на банки	11
Подмена документов на АРМ КБР	17
Обеспечение живучести трояна	19
Утечка исходных кодов	22
Рекомендации	24
Индикаторы	26

В ежегодном [отчете о тенденциях развития высокотехнологичных преступлений](#) мы отмечали рост интереса преступников к хищениям у финансовых организаций и прогнозировали увеличение количества целевых атак в 2016 году.

Мы уже публиковали открытые отчеты о тактиках таких групп как [Anunak](#) (также известной как Carbanak), [Corkow](#) (также известной как Metel), «специализирующихся» на финансовых учреждениях. Buhtrap, о которой пойдет речь ниже, является ярким примером эволюции преступной группы, перешедшей от атак на клиентов банков — к атакам непосредственно на банки.

Во многом благодаря ее активности атаки на российские банки, результатом которых является прямой ущерб в сотни миллионов рублей, перестали восприниматься как что-то необычное.

Основная причина успеха Buhtrap — **плохая осведомленность о процессе проведения целевых атак на финансовый сектор**: участники рынка не понимают, как именно реализуются

атаки, и поэтому не могут выработать адекватные меры противодействия.

С этим связана и вторая причина — **излишняя вера в то, что стандартные средства защиты**, такие как лицензионный и обновленный антивирус, последняя версия операционной системы, использование межсетевых экранов или средств предотвращения утечек (DLP), остановят злоумышленников на одном из этапов развития атаки.

Целью данного отчета является **повышение осведомленности** банковского сообщества о тактике действий злоумышленников, **предоставление индикаторов** для выявления попыток компрометации корпоративной сети **и рекомендаций**, которые помогут противостоять действиям преступников.

Группа Buhtrap действует с октября 2014 года, однако первые атаки на финансовые учреждения были зафиксированы в августе 2015 года. До этого группа атаковала только клиентов банков. Фокус атаки в настоящее время приходится на банки России и Украины.

600 миллионов ₺

максимальная сумма хищения у российского банка (2016)

25,6 миллионов ₺

минимальная сумма хищения у российского банка (2015)

143 миллиона ₺

средняя сумма успешного хищения у банка

1 миллиард ₺

сумма хищения, которое удалось остановить в январе 2016

Атаки Buhtrap представляют угрозу для финансовой устойчивости жертв:

62%

среднее отношение суммы успешного хищения к уставному капиталу банка

в 2,5 раза

сумма хищения превысила размер уставного капитала банка в двух случаях

С августа 2015 года по февраль 2016 группа Buhtrap совершила **13 успешных атак на банки России** на общую сумму **в 1,8 миллиарда рублей**. Количество успешных атак на банки Украины не установлено.

Buhtrap — первая преступная группа, начавшая использовать сетевого червя для поражения всей инфраструктуры банка,

что значительно усложняет процесс очистки сети.

В результате банкам приходится отключать всю инфраструктуру, что приводит к простоям в обслуживании клиентов и дополнительным издержкам.

Вредоносные программы целенаправленно ищут машины с автоматизированным рабочим местом клиента Банка России (далее — АРМ КБР). Мы не обнаружили инцидентов с системами мгновенных денежных переводов, банкоматами или платежными шлюзами, которые интересуют участников других преступных групп.

Основным вектором проникновения в корпоративные сети являются фишинговые письма от имени Банка России или его представителей, однако мы также зафиксировали распространение через наборы эксплойтов (с использованием инфраструктуры преступной группы [Corkow](#) (Metel)) и дистрибутивы легального программного обеспечения.

В феврале 2016 года в открытом доступе были опубликованы исходные коды вредоносной программы, что привело к ее широкому распространению. **Публикация исходных кодов может привести к появлению новых модификаций этой вредоносной программы** и увеличению количества аналогичных инцидентов.

Абсолютно все инциденты можно было легко предотвратить. Годовые затраты на эффективные средства предотвращения в 28 раз меньше, чем средний прямой ущерб от одной целенаправленной атаки.

20 октября 2014 года мы уведомили подписчиков системы киберразведки Threat Intelligence о рассылке писем с адреса электронной почты **info@beeline-mail.ru** с темой **«Счет № 522375-ФЛОРЛ-14-115»** (рис. 1). Доменное имя beeline-mail.ru было зарегистрировано также 20 октября 2014 года.

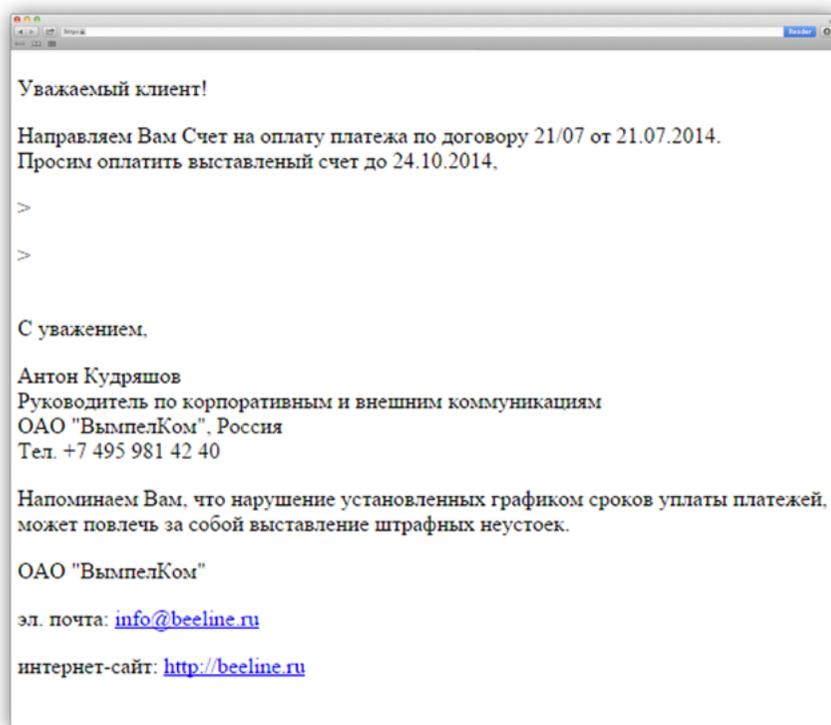


Рисунок 1. Снимок экрана фишингового письма от имени компании ОАО «ВымпелКом»

В приложении к письму находился специальным образом сформированный **RTF-документ, эксплуатирующий уязвимость CVE-2012-0158 в библиотеке «MSCOMCTL.OCX»**. Этой уязвимости подвержены все версии MS Word, начиная с версии 2003.

21 ноября 2014 года аналогичная рассылка была осуществлена с почтового ящика **info@extern-kontur.ru** с темой письма **«Оплата услуг СКБ Контур»** от имени ЗАО «ПФ «СКБ Контур»» (рис. 2), занимающегося разработкой программного обеспечения для электронного документооборота, бухучета и управления предприятием.

ЗАРАЖЕНИЕ

При открытии RTF-файла в каталоге «%User%» создавался файл «ntxobj.exe», который прописывался в автозагрузку и запускался, устанавливая загрузчик NSIS (Nullsoft Scriptable Install System — система создания установочных программ для Microsoft Windows с открытыми исходными кодами) с разными модулями и скриптами.

Вредоносные модули представляли собой самораспаковывающиеся архивы формата 7z, защищенные паролем. Многие модули были подписаны действительными цифровыми сертификатами.

Если скрипты обнаруживали, что программа запущена под отладкой, на виртуальной машине или на компьютере, не имеющем поддержку русского языка, она завершала свою работу.

Если условия, необходимые для работы программы, соблюдались, производился поиск по файлам и папкам по следующим подстрокам: «iBank2», «amicon», «bifit» «bss», «ibank», «gpb», «inist», «mdm», «Aladdin», «Amicon», «Signal-COM», «bc.exe», «intpro.exe», «cfta», «agava», «R-Style», «AKB», «Perm» «AKB Perm», «CLUNION.0QT», «ELBA». Кроме того, скрипты искали исполняемые файлы, имеющие отношение к банковским приложениям разных производителей (см. перечень на стр. 7).

ПОЛУЧЕНИЕ ДАННЫХ

Основной модуль с названием исполняемого файла rp_rack.exe специализируется на краже данных и взаимодействии с удаленным командным сервером. Его запуск выполняется с использованием известного продукта **Yandex Punto** и позволяет отслеживать и передавать на удаленный сервер нажатие клавиш (кейлоггер) и содержимое буфера обмена, а также перечислять смарт-карты, присутствующие в системе.

УДАЛЕННОЕ УПРАВЛЕНИЕ

Если вредоносная программа подтверждала наличие банковских приложений, злоумышленники по команде загружали на компьютер легитимное средство удаленного управления **Lite Manager**.

Для управления зараженным компьютером использовались программы с исполняемыми файлами mimi.exe и xtm.exe. Они позволяют получить или восстановить пароль от всех активных учетных записей Windows за весь период работы с момента включения, создать новый аккаунт в операционной системе,

включить сервис RDP (Remote Desktop Protocol). После успешного подключения злоумышленники создавали мошеннические платежные поручения и отправляли их в банк на исполнение.

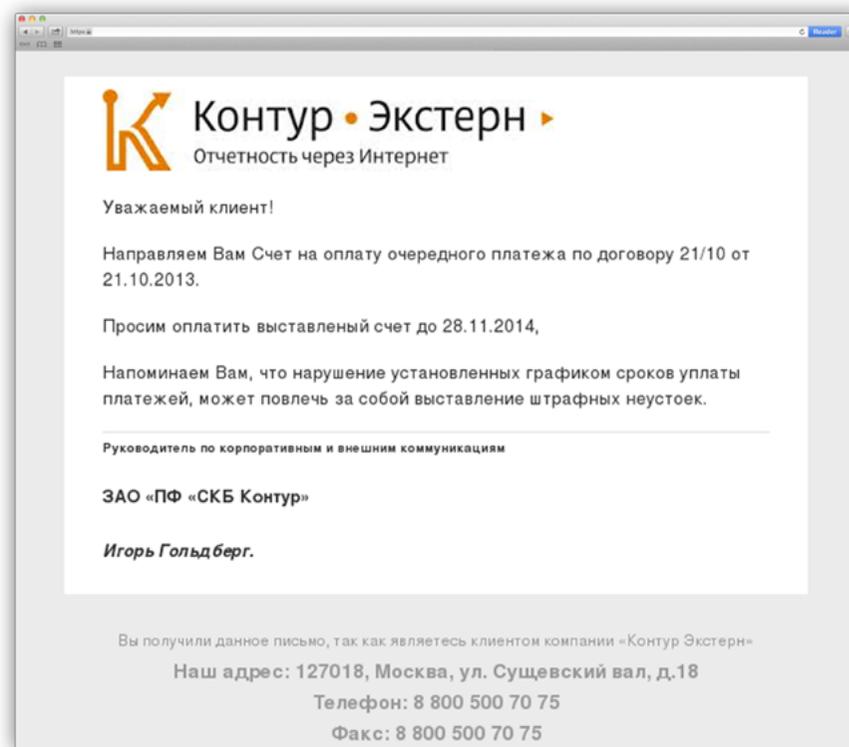


Рисунок 2. Снимок экрана фишингового письма от имени компании ЗАО «ПФ «СКБ Контур»»

ИСПОЛНЯЕМЫЕ ФАЙЛЫ, НАЛИЧИЕ КОТОРЫХ ПРОВЕРЯЕТ ВУНТРАР

ip-client.exe,
prclient.exe, rclient.exe,
saclient.exe,
SRCLBClient.exe,
twawebclient.exe,
vegaClient.exe,
dsstart.exe,
dtpaydesk.exe,
eelclnt.exe, elbank.exe,
etprops.exe, eTSrv.exe,
ibconsole.exe,
kb_cli.exe, KLBS.exe,
KlientBnk.exe,
lfcpaymentais.exe,
loadmain.exe, lpbos.exe,
mebiusbankxp.exe,
mmbank.exe,
pcbank.exe, pinpayr.exe,
Pionner.exe,
pkimonitor.exe,
pmodule.exe, pn.exe,
postmove.exe,

UpMaster.exe,
SGBClient.exe,
el_cli.exe,
MWClient32.exe,
ADirect.exe,
BClient.exe, bc.exe,
ant.exe, arm.exe,
arm_mt.exe,
ARMSH95.EXE,
asbank_lite.exe,
bank.exe, bank32.exe,
bbms.exe, bk.exe,
BK_KW32.EXE,
bnk.exe, CB.exe,
cb193w.exe, cbank.exe,
cbmain.ex,
CBSMAIN.exe,
CbShell.exe, clb.exe,
CliBank.exe,
CliBankOnlineEn.exe,
CliBankOnlineRu.exe,
CliBankOnlineUa.exe,

client2.exe, client6.exe,
clientbk.exe, clntstr.exe,
clntw32.exe,
contactng.exe, Core.exe,
cshell.exe,
cyberterm.exe,
client.exe, cncclient.exe,
bbclient.exe,
EximClient.exe,
fcclient.exe, iscc.exe,
kabinet.exe,
SrCLBStart.exe,
srcbclient.exe,
Upp_4.exe,
Bankline.EXE,
GeminiClientStation.exe,
ClientBank.exe,
ISClient.exe, cws.exe,
CLBANK.EXE,
IMBLink32.exe,
cbsmain.dll,
GpbClientSftcws.exe,

quickpay.exe, rclaunch.exe,
retail.exe, retail32.exe,
translink.exe, unistream.exe,
uralprom.exe, w32mkde.exe,
wclnt.exe, wfinist.exe,
winpost.exe, wupostagent.exe,
Zvit1DF.exe, BC_Loader.exe,
Client2008.exe,
lbcRemote31.exe, _ftcgpk.exe,
scardsvr.exe, CL_1070002.exe,
intpro.exe, Run.exe,
SGBClient.ex, sx_Doc_ni.exe,
icb_c.exe, Client32.exe,
BankCl.exe,
ICLTransportSystem.exe,
GPBClient.exe, CLMAIN.exe,
ONCBCLI.exe, rmclient.exe,
RkcLoader.exe, CLBank3.exe,
FColseOW.exe,
productprototype.exe,

ТАКТИКА АТАК BUHTRAP НА КЛИЕНТОВ БАНКОВ

1. Покупались доменные имена, схожие по написанию с доменами легитимных компаний, от имени которых планировалось проводить атаки.
2. Арендовался сервер, на котором был корректно настроен почтовый сервер для рассылки фишинговых писем от имени легитимной компании. Корректная настройка отдельного сервера и покупка схожих по написанию доменов были необходимы, чтобы снизить вероятность попадания в спам и повышения вероятности открытия приложенных файлов.
3. После успешного запуска вредоносной программы в результате эксплуатации уязвимостей проверялось наличие установки на системе поддержки русского языка и отсутствие признаков запуска в виртуальной или отладочной среде с целью снизить риск быть обнаруженными средствами защиты и антивирусными компаниями.
4. Запускался основной модуль вредоносной программы, отвечающий за сбор данных и отправку их на удаленный сервер атакующего.
5. Вредоносная программа осуществляла поиск файлов и иных следов, характерных для работы с банковскими приложениями. Их подробный список мы привели выше.
6. Если работа с банковскими приложениями была зафиксирована, по команде осуществлялась загрузка легитимного средства удаленного доступа Lite Manager. Операционная система настраивалась таким образом, чтобы доступ по протоколу RDP был разрешен.
7. Используя удаленный доступ, злоумышленники создавали мошеннические платежные поручения и отправляли их в банк.

Подготовка к распространению фишинговых писем, проверка окружения и организация удаленного доступа напоминали хорошо подготовленную **целенаправленную атаку, схожую по тактике с действиями группы Anunak**, преуспевшей в хищениях у банков.

Максимальная сумма хищения Buhtrap у юридического лица — клиента банка составила 40 миллионов рублей, в то время как [Anunak](#) зарабатывала на банках сотни миллионов. Смена целей, ставшая очевидной осенью 2015 года, была вполне закономерна.

Группа активно атаковала клиентов банков, вкладывалась в доработку вредоносной программы и искала более эффективные способы ее распространения по корпоративным сетям. Нами было зафиксировано три разных способа распространения Vuhtrap.

ФИШИНГОВЫЕ РАССЫЛКИ

Основной способ распространения Vuhtrap, использовавшийся для атак как на клиентов банков, так и на сами банки,

о чем мы расскажем ниже.

Если документ распространялся без эксплойта (CVE-2012-0158, CVE-2013-3906 и CVE-2014-1761), но с макросами, в документе находилась инструкция по их включению (рис.3). Следование инструкциям по запуску макроса приводило к загрузке Vuhtrap.

Иногда злоумышленники распространяли вредоносный исполняемый файл непосредственно в зашифрованных архивах.

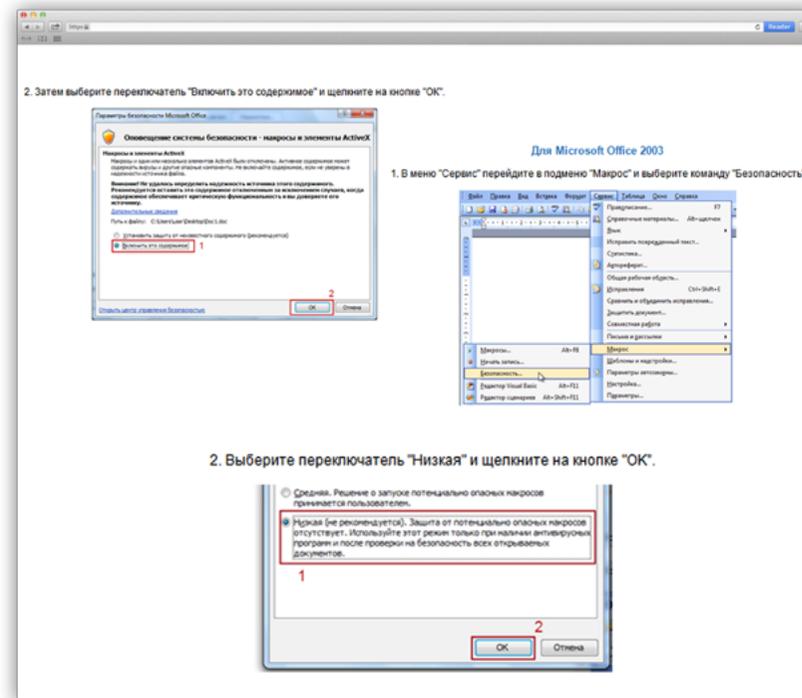
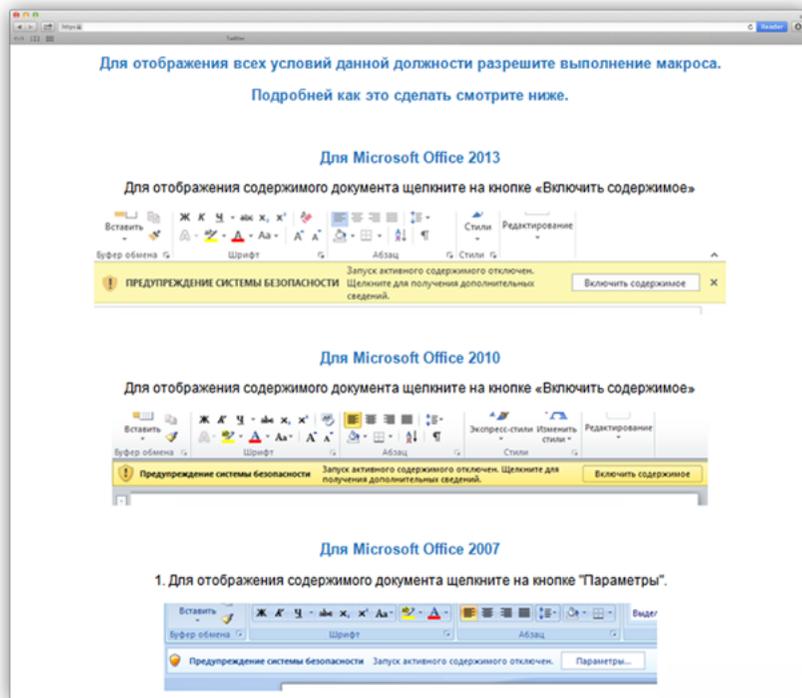
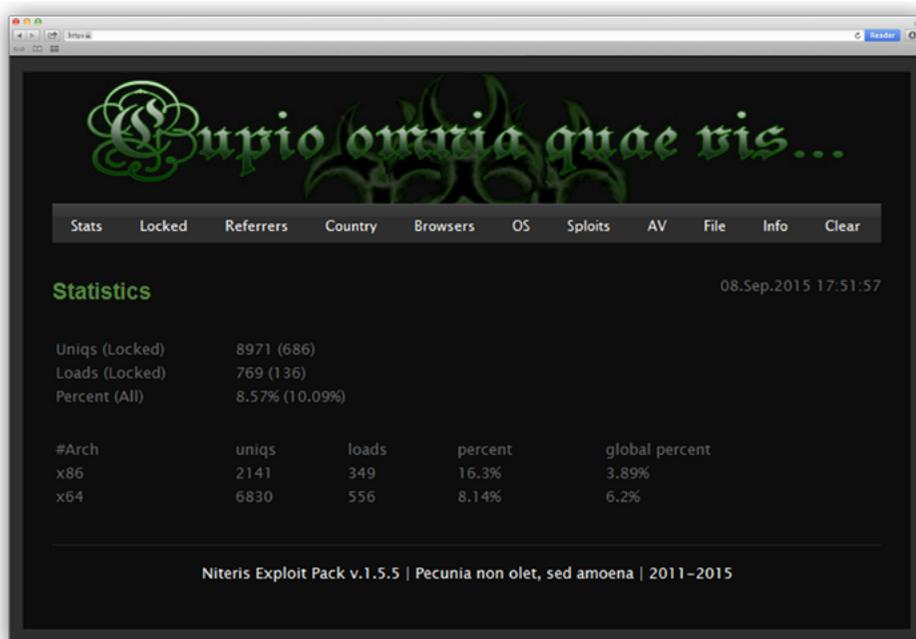


Рисунок 3. Инструкция по включению макросов при открытии вредоносного документа

НАБОРЫ ЭКСПЛОЙТОВ

Мы фиксировали распространение Buhtrap подобным способом с мая по август 2015 года. Пользователь заходил на взломанный легальный ресурс, с которого его в скрытом режиме перенаправляли на сервер с набором эксплойтов. В случае успешной эксплуатации уязвимостей на компьютер загружался Buhtrap.

Среди взломанных легальных сайтов — бухгалтерские порталы, сайты, посвященные регистрации юридических лиц, и сайты, посвященные строительству.



Примечательно, что для распространения Buhtrap использовались те же взломанные сайты, что и для трояна Corkow. Более того, использовался тот же набор эксплойтов **Niteris** (рис.4), что и в Corkow. Это может свидетельствовать о том, что участники этих преступных групп поддерживают связь.

ЛЕГАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

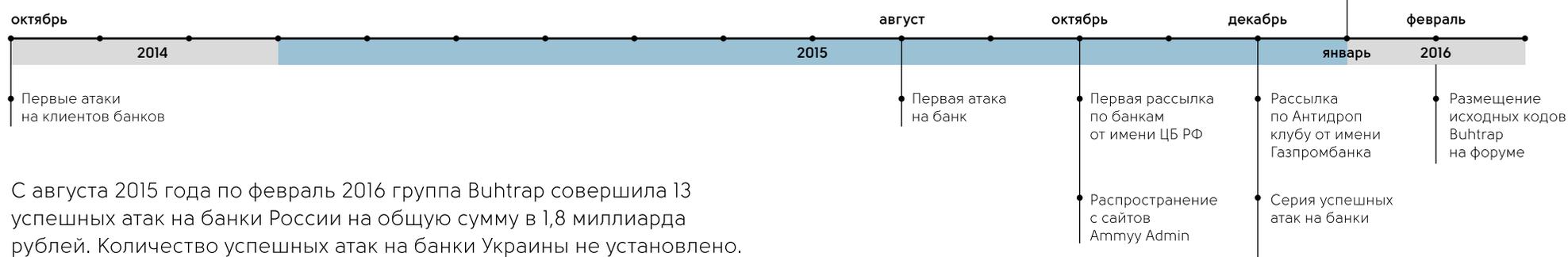
В конце октября аналитики компании Eset Nod32 заметили вредоносную активность на сайте компании **Ammyy**, которая специализируется на разработке инструмента удаленного доступа **Ammyy Admin**. Злоумышленникам удалось загрузить на сервер веб-сайта компании вредоносную модификацию дистрибутива этой программы, которая содержала троян Buhtrap.

Стоит отметить, что в разные периоды времени с этого сайта распространяли модифицированную версию **Ammyy** не только с Buhtrap, но и другими троянами: Lurk, CoreBot, Ranbyus, Netwire RAT.

Рисунок 4. Система управления набором эксплойтов Niteris (также известная как CottonCastle)

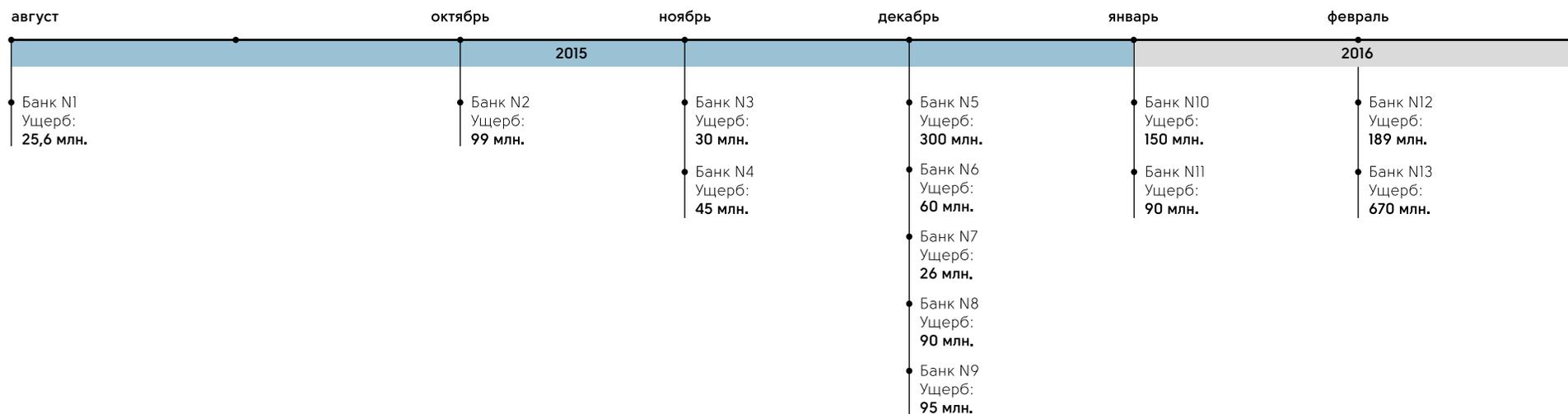
Первые успешные атаки на банки мы зарегистрировали чуть раньше чем через год после первых атак на клиентов банков.

Хронология развития группы Buhtrap



С августа 2015 года по февраль 2016 группа Buhtrap совершила 13 успешных атак на банки России на общую сумму в 1,8 миллиарда рублей. Количество успешных атак на банки Украины не установлено.

Хронология успешных атак на банки



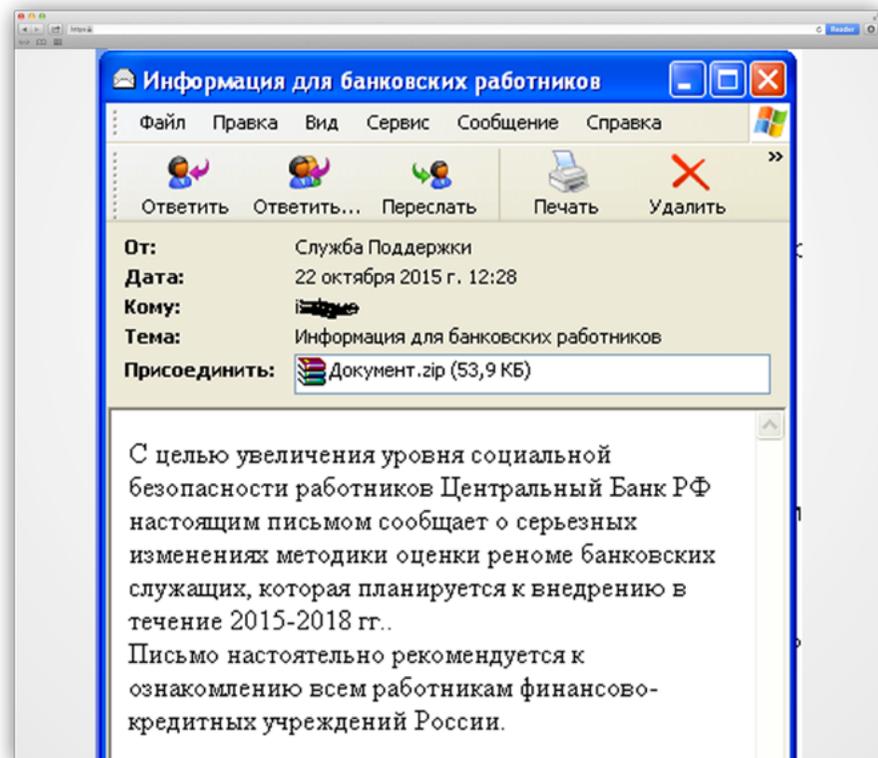
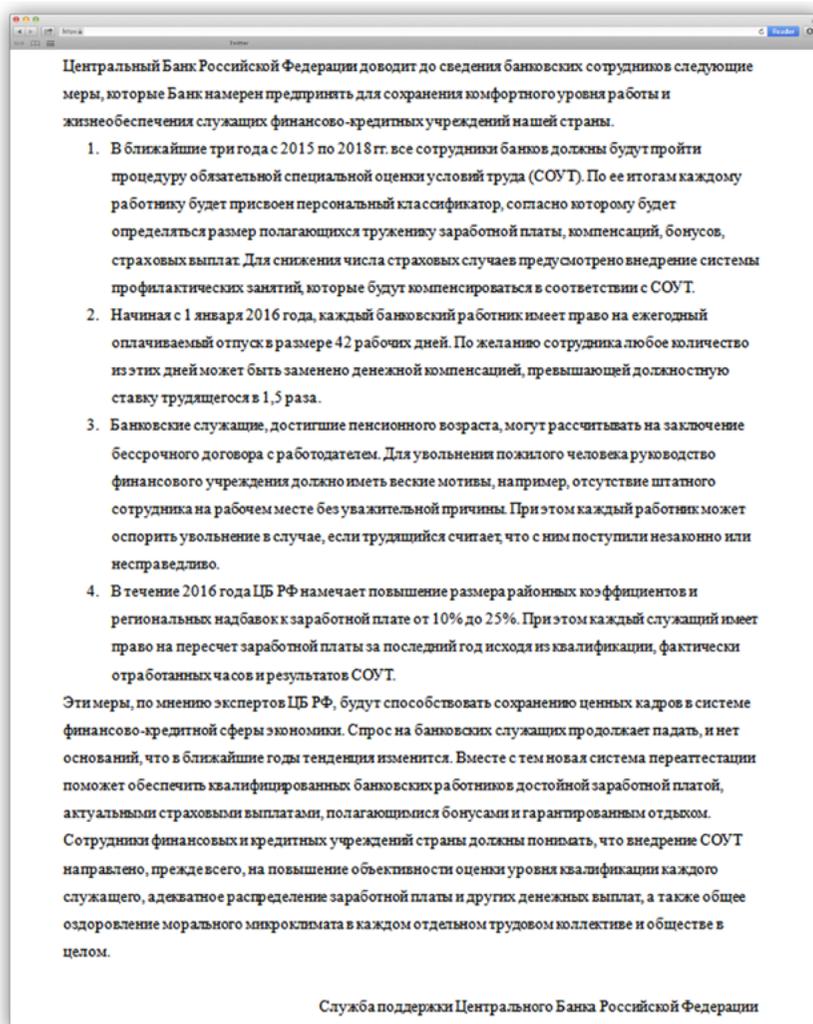


Рисунок 5. Снимок экрана фишингового письма от имени ЦБ РФ

ПЕРВАЯ РАССЫЛКА ОТ ИМЕНИ БАНКА РОССИИ

22 октября 2015 года мы уведомили клиентов системы киберразведки Threat Intelligence о рассылке писем от имени Центрального банка РФ с почтового ящика **support@cbr.ru.com** с темой «**Информация для банковских работников**» (рис. 5). Рассылка была массовой, многие российские банки подтвердили получение этого письма.

В приложении к письму находился ZIP-архив, содержащий документ MS Office (рис. 6). Открытие документа приводило к запуску скрипта, проверявшего в истории браузеров наличие переходов по ссылкам, связанным с интернет-банками и банковским программным обеспечением.



Если такие ссылки обнаруживались, то программа загружала из интернета вредоносное программное обеспечение (сервер удаленного доступа LiteManager, кейлоггер и основной модуль Vu-htrap) и устанавливала его.

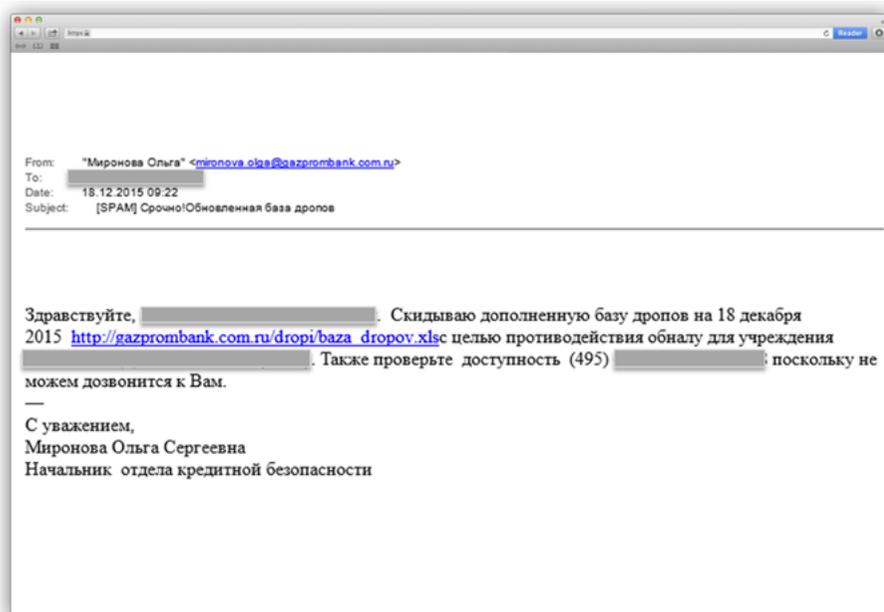
Стоит отметить, что **большинство антивирусных программ не определяет загрузчик как вредоносную программу**, а все загружаемые программы имели валидную цифровую подпись.

Рисунок 6. Распакованный документ из фишингового письма от имени ЦБ РФ

РАССЫЛКА ПО УЧАСТНИКАМ КЛУБА «АНТИДРОП»

Рассылка фишинговых писем от имени регулятора уже является стандартной практикой. Однако участники группы Buhtrap пошли дальше.

Они узнали о наличии так называемого клуба «Антидроп», куда входят специалисты по безопасности из нескольких сотен банков. Участники этого клуба обмениваются информацией, которая позволяет им выявлять и блокировать мошеннические операции.



Предположительно в результате одной из первых атак на банки они получили список рассылки клуба «Антидроп» и сделали специальное фишинговое письмо для его участников.

18 декабря 2015 группа Buhtrap начала проводить рассылку писем с адреса электронной почты mironova.olga@gazprombank.com.ru с темами: **«Срочно! Обновленная база дропов»**, **«Обновленная база дропов»** (рис. 7). В письме содержалась ссылка на вредоносный файл, размещенный на ресурсе с мошенническим доменом gazprombank.com.ru.

Переход по ссылке приводил к загрузке документа, при открытии которого запускалась цепочка процессов, аналогичная сценарию с письмами от имени ЦБ РФ.

Сотрудники безопасности банков достаточно быстро поняли, что рассылка является мошеннической, и довели это до сведения всех участников клуба, ввиду чего ее эффективность сразу была сведена к нулю.

Рисунок 7. Снимок экрана фишингового письма от имени Газпромбанка

ВТОРАЯ РАССЫЛКА ОТ ИМЕНИ БАНКА РОССИИ

В январе 2016 преступники вернулись к схеме отправки писем от имени Банка России, но уже с предложением о трудоустройстве.

Так 29 января 2016 года система киберразведки Threat Intelligence зафиксировала адреса **vakansiya@cbr.ru.net** с темой «**Вакансия в Центральном Банке РФ**» (рис. 8). В приложении к письму был документ MS Office «Вакансия_34.doc», содержащий инструкцию по включению макросов. В случае успешного выполнения макросов демонстрировался текст вакансии. Пример инструкции приведен в разделе «Способы распространения».

Включение макросов приводило к проверке системы жертвы. Если языком системы был русский или украинский, а также выполнялся ряд

других условий, то загружался и запускался файл из архива Buhtrap.

Файл устанавливал программу удаленного доступа **LiteManager** и программу **Guide**, с помощью которой подгружался основной модуль. Этот модуль выполняет команды управляющего сервера на загрузку и исполнение программ, устанавливает клавиатурный шпион и перечисляет смарт-карты. Сама программа Guide является легитимной и используется для создания документов.

После успешного заражения хотя бы одного из хостов в результате фишинговой рассылки атакующие запускали вредоносную программу, действующую по принципу червя, которую мы назвали **BuhTrapWorm**. Именно он обеспечивал максимальную живучесть в системе.

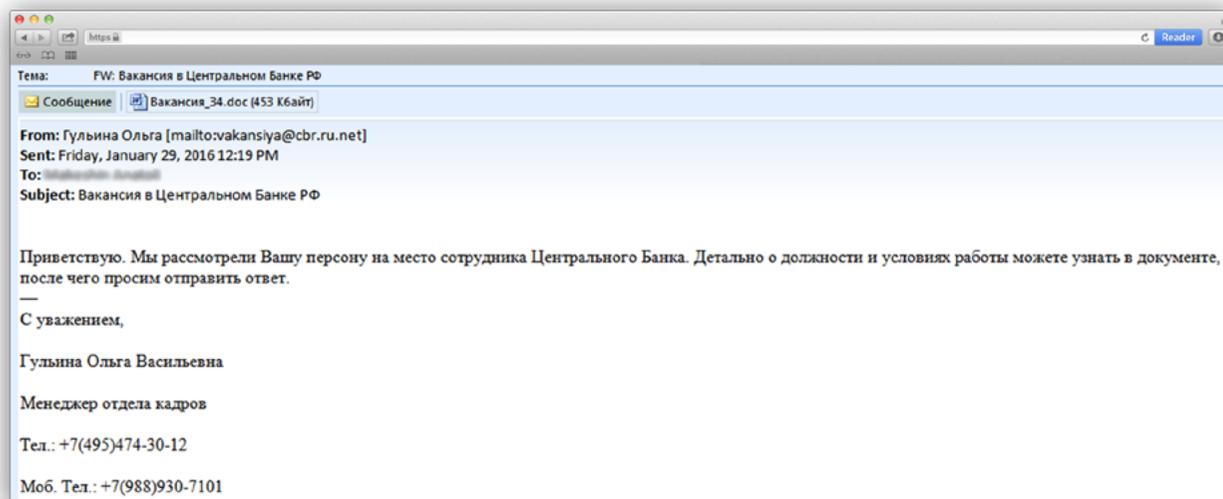


Рисунок 8. Снимок экрана фишингового письма от имени ЦБ РФ

ТАКТИКА АТАК BUHTRAP НА БАНКИ

1. После первичного попадания во внутреннюю сеть банка с помощью удаленного доступа загружался и запускался модуль, отвечающий за живучесть трояна и заражение множества хостов внутри банка.
2. С помощью модифицированного варианта Mimikatz осуществлялся сбор логинов и паролей от доменных учетных записей.
3. Производился поиск системы с установленным программным обеспечением АРМ КБР.
4. После получения доступа к АРМ КБР осуществлялась подмена платежных документов в адрес Банка России, который их исполнял.
5. Выводились из строя зараженные рабочие станции внутри банка, чтобы усложнить сбор доказательной базы.

В случае с Buhtrap мы видим, что **злоумышленники всегда ищут именно рабочие места с АРМ КБР**. Мы не обнаружили инцидентов с системами мгновенных денежных переводов, банкоматами или платежными шлюзами, которые интересуют участников других преступных групп.

Отдельно стоит рассмотреть процесс подмены платежных поручений на АРМ КБР, так как многие банки уделяют недостаточно внимания защите этого программного обеспечения.

Автоматизированное рабочее место клиента Банка России (АРМ КБР) – программный комплекс для отправки платежных документов от банка в ЦБ РФ в унифицированных форматах электронных банковских сообщений (УФЭБС) рейсами.

АРМ КБР распространяется свободно на сайте Центрального Банка, любой пользователь может загрузить его и протестировать особенности работы программы.

Процедура начального конфигурирования выполняется при первом запуске АРМ. Она включает в себя установку параметров хранилищ платежных документов и добавление пользователей.

Параметры хранилищ зафиксированы в файле с именем вида <имя компьютера>.cfg в подкаталоге cfg каталога, в который установлен АРМ КБР. Файл конфигурации в формате XML доступен для чтения каждому, кто подключается к АРМ КБР.

При установке может быть указан способ хранения платежных документов:

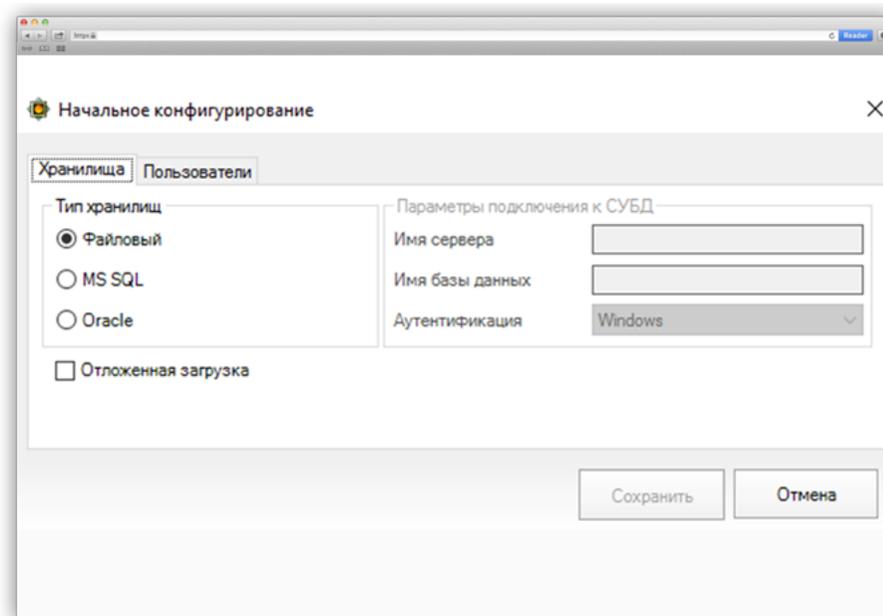
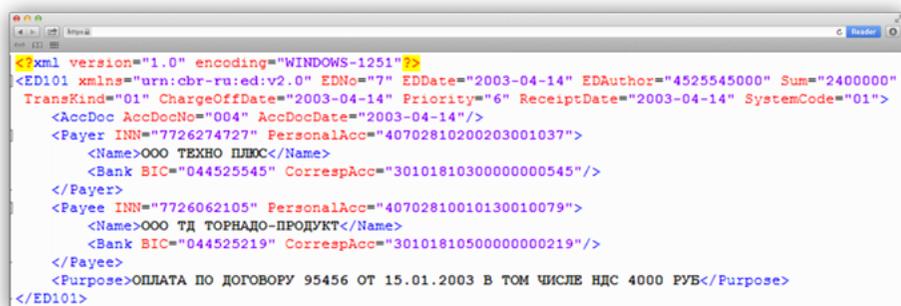


Рисунок 9. Выбор типа хранилища УФЭБС

В инцидентах, расследуемых Group-IB, был выбран «файловый» тип хранения. Это значит, что электронные сообщения в формате УФЭБС (описание которого также находится в открытом доступе на сайте ЦБ), хранятся в заданном при конфигурации каталоге и автоматически забираются для обработки программным обеспечением АРМ КБР. Пример платежного рейса приведен ниже:



```
<?xml version="1.0" encoding="WINDOWS-1251" ?>
<ED101 xmlns="urn:cbr-ru:ed:v2.0" EDNo="7" EDDate="2003-04-14" EDAuthor="4525545000" Sum="2400000"
TransKind="01" ChargeOffDate="2003-04-14" Priority="6" ReceiptDate="2003-04-14" SystemCode="01">
  <AccDoc AccDocNo="004" AccDocDate="2003-04-14"/>
  <Payer INN="7726274727" PersonalAcc="40702810200203001037">
    <Name>ООО ТЕХНО ПЛЮС</Name>
    <Bank BIC="044525545" CorrespAcc="30101810300000000545"/>
  </Payer>
  <Payee INN="7726062105" PersonalAcc="40702810010130010079">
    <Name>ООО ТД ТОРНАДО-ПРОДУКТ</Name>
    <Bank BIC="044525219" CorrespAcc="30101810500000000219"/>
  </Payee>
  <Purpose>ОПЛАТА ПО ДОГОВОРУ 95456 ОТ 15.01.2003 В ТОМ ЧИСЛЕ НДС 4000 РУБ</Purpose>
</ED101>
```

Рисунок 10. Пример документа в формате УФЭБС

Таким образом, для формирования платежного рейса злоумышленнику необходим логин и пароль для доступа к каталогу, из которого АРМ КБР забирает файлы для обработки. Он может **скопировать содержимое предыдущего рейса и заменить содержание необходимых полей**. Так и происходило в наблюдаемых нами случаях.

При других способах хранения платежных документов преступнику необходим логин и пароль на доступ в соответствующую базу данных. В остальном процедура формирования рейса аналогична.

Кроме того, злоумышленник может **добавить свое платежное поручение в уже сформированный рейс**, исправив содержимое соответствующего файла или записи в базе данных.

Следуя рекомендациям ЦБ, также опубликованным на сайте регулятора, банк может использовать программное обеспечение **СКАД «Сигнатура»**, которое проверяет целостность АРМ КБР и позволяет подписывать платежные документы, отправляемые в ЦБ. Однако оно **не поможет предотвратить такую атаку**: подмена платежных документов никак не нарушает целостность АРМ КБР, и программа, по сути, защищает уже измененные злоумышленниками документы.

Само программное обеспечение АРМ КБР не проверяет целостность документов для отправки, а также достоверность данных отправителя и получателя платежей. Таким образом, формирование рейса злоумышленником происходит до его поступления в АРМ КБР.

При этом ему даже не обязательно указывать достоверные данные.

С августа 2015 года в сетях организаций, зараженных вредоносной программой Buhtrap, нами замечено использование новой вредоносной программы, действующей по принципу червя, которую мы назвали **BuhtrapWorm**.

ЭТАПЫ РАСПРОСТРАНЕНИЯ BUHTRAPWORM

1. Для начала распространения программы в сети организации необходимо запустить основной модуль на одном из компьютеров сети, к которому осуществляются подключения под учетной записью администратора домена.

Основной модуль выполняется и хранится в оперативной памяти компьютера. Посредством чтения памяти процесса «lsass.exe» он извлекает логины и соответствующие им пароли для всех клиентских сессий на текущем компьютере (работа схожа с функциональными возможностями утилиты **Mimikatz**).

Модуль проводит сканирование сети на наличие на компьютерах объекта mailslot с заданным именем «**\\.\mailslot\46CA075C-165CBV2786**». Объект с таким именем служит индикатором зараженности.

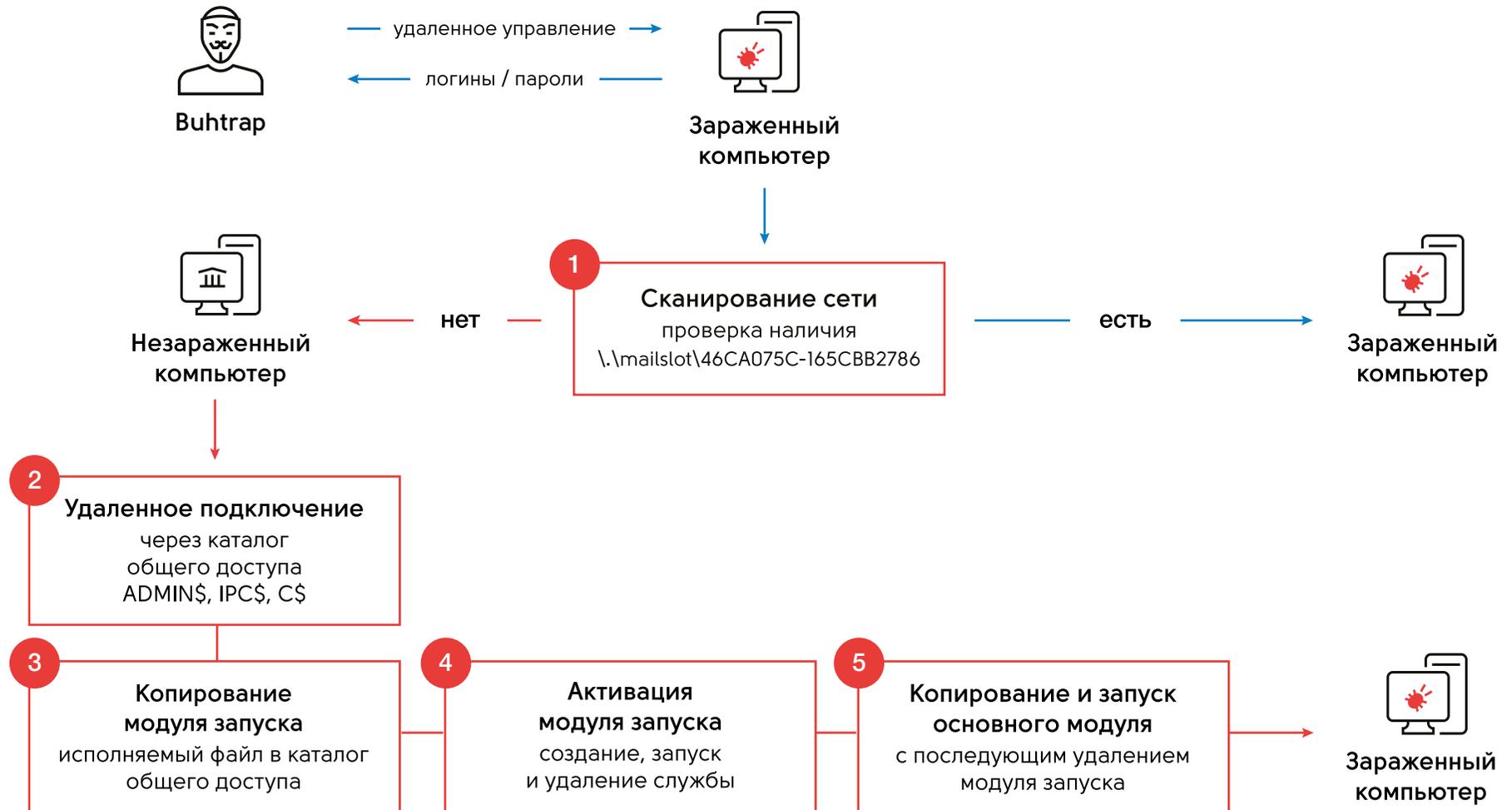
2. Если он отсутствует, проводится подключение к компьютеру посредством каталога общего доступа с использованием

извлеченных пар логин-пароль. В качестве каталогов общего доступа могут использоваться «\ADMIN\$», «\ipc\$», «\C\$».

3. Если подключение проведено успешно, в этот каталог (по умолчанию таким каталогом является «C:\WINDOWS») копируется модуль запуска в виде исполняемого файла.
4. Далее на незараженном компьютере создается служба со случайным именем, в свойствах которой прописывается путь к модулю запуска. С зараженного компьютера на незараженный посылается команда на запуск службы, активирующая модуль. После этого служба удаляется из системы.
5. Модуль запуска копирует с зараженного компьютера основной модуль в файл с именем вида: «<имя модуля запуска>.dat» или в объект pipe с заданным именем (уникальным для каждого компьютера). После запуска основного модуля модуль запуска удаляется из системы с перезаписью содержимого файла.

После заражения нового компьютера распространение вредоносной программы производится по той же схеме. Таким образом, **за считанные минуты образуется самоподдерживающаяся бот-сеть внутри корпоративной сети.**

ЭТАПЫ РАСПРОСТРАНЕНИЯ BUHTRAPWORM



Основной модуль не только содействует распространению червя, но и осуществляет использование уязвимости операционной системы для повышения прав и привилегий в системе, а также соединение с сервером управления, обеспечивая возможность удаленного подключения по протоколу RDP к зараженному компьютеру. Каждый зараженный компьютер сети доступен извне по протоколу RDP.

После перезагрузки компьютера содержимое оперативной памяти очищается вместе с модулем полезной нагрузки. Таким образом, **при наличии хотя бы одного компьютера в сети организации, зараженного вредоносной программой BuhtrapWorm, все остальные компьютеры будут заражаться снова и снова после перезагрузки.**

На сегодняшний момент антивирусными программами детектируется только модуль запуска, который сам по себе не представляет угрозы. Более того, его удаление не влечет за собой удаление вредоносной программы с компьютера.

В случае ошибок в работе вредоносной программы может не произойти остановка, удаление службы или модуля запуска, и они могут сохраняться в зараженной системе в большом количестве.

05.02.2016 на андеграундном ресурсе «exploit.in» было опубликовано объявление со ссылкой на скачивание исходного кода Buhtrap (рис.11). По словам автора, он является одним из участников команды Buhtrap. Однако в связи с тем, что ему как разработчику не заплатили за проект, он решил выложить все исходные коды вредоносной программы в открытый доступ. Коды были запакованы в RAR-архив с паролем и выложены на файловом хранилище Sendspace.

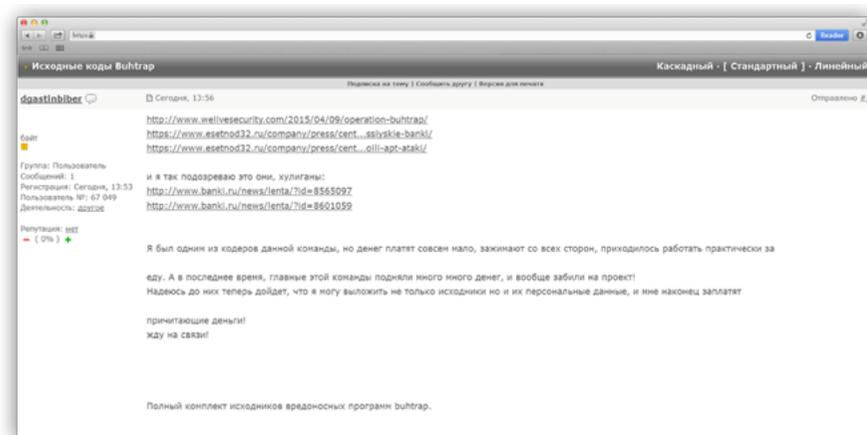


Рисунок 11. Сообщение на хакерском форуме с исходными кодами Buhtrap

Исходя из содержимого архива, данная версия исходных кодов группы Buhtrap относится к промежутку лето — начало осени 2015 года. Об этом говорит отсутствие в архиве кодов модуля «rsxhex», а также других программ, задействованных в последних преступлениях данной группы.

Выложенные исходные коды являются рабочими. Их широкое распространение может привести к увеличению количества инцидентов с использованием этой вредоносной программы, но уже другими преступными группами. Интерфейс билдера показан на рисунке ниже.

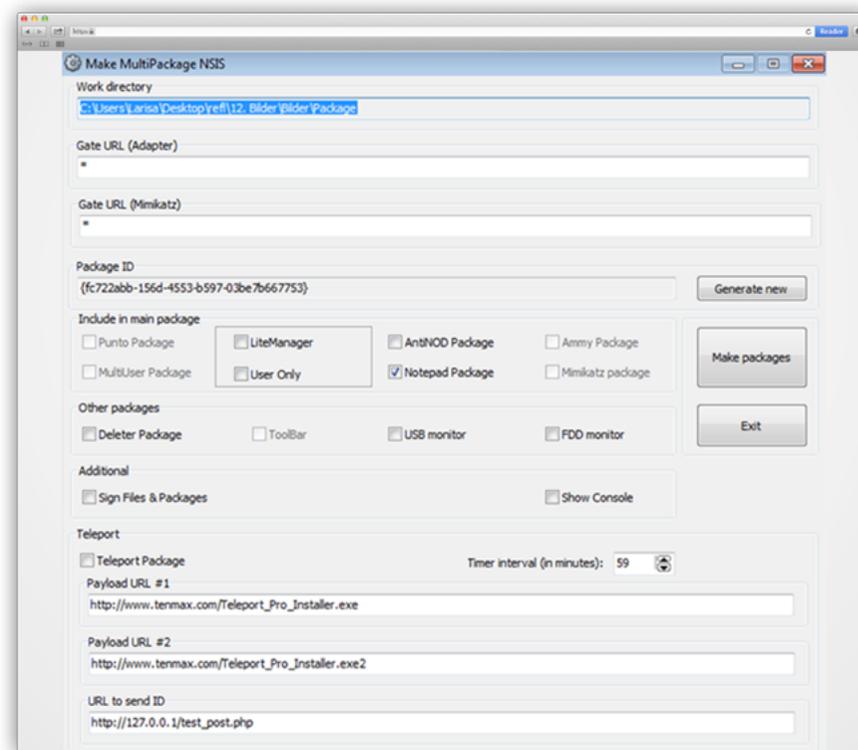


Рисунок 12. Снимок экрана билдера Buhtrap

ОПУБЛИКОВАННЫЕ МОДУЛИ:

- **ВНО** — модуль для подмен страниц в браузере Internet Explorer.
- **kill_os** — модуль для уничтожения загрузочных записей MBR. Предусмотрен вариант срабатывания после определенных действий в системе. «Damagewindow» — фейковое окно, которое запускается после повреждения записи MBR, с просьбой перезагрузить систему в связи с внутренней ошибкой.
- **loaders** — билдеры NSIS-скриптов для установки вредоносного программного обеспечения. Предусмотрен вариант открытия документов после успешного исполнения.
- **mimimod** — модифицированная программа mimikatz, используемая для получения учетных записей пользователей в системе.
- **ID** — алгоритм вычисления уникального номера зараженной машины.
- **BSShide** — модуль скрытия платежных поручений в системе BSS. Модифицирует страницу, отображаемую пользователю.
- **antidetekt** — модуль обнаружения виртуального окружения, песочниц.
- **UAC** — модуль обхода защиты UAC.
- **RDP** — модифицирование ОС с целью возможной одновременной работы нескольких пользователей в системе.
- **VNC** — удаленное управление ПК с бэкконектом.
- **DLL Side-Loading** — основной модуль. Устанавливает клавиатурный шпион, считыватель смарт-карт в систему, обеспечивает связь с административной панелью и установку и работу других модулей в системе. По заявлению автора, содержит обход антивирусных программ и фаерволов.
- **Панель управления.**
- **Билдер** — программа для сбора модулей в единый исполняемый файл.

Также данный архив содержит несколько сборок **связки эксплойтов MWI**. Сборки сгруппированы по эксплуатации различных уязвимостей:

- CVE-2012-0158, CVE-2010-3333
- CVE-2013-3906, CVE-2012-0158, CVE-2010-3333
- CVE-2014-1761, CVE-2013-3906, CVE-2012-0158, CVE-2010-3333

Абсолютно все целенаправленные атаки на банки можно было выявить и остановить на разных этапах развития. Ниже мы приводим простые рекомендации, которые позволят более эффективно противостоять атакующим.

ПРЕДОТВРАЩЕНИЕ НА ЭТАПЕ ПРОНИКНОВЕНИЯ

Основным способом проникновения в банковскую сеть является отправка фишингового письма с вложением, которое содержит эксплойт, документ с макросом или исполняемый файл в архиве с паролем.

Чтобы предотвратить заражение в результате работы эксплойта, достаточно производить обновление программного обеспечения Microsoft. Эта преступная группа не использовала уязвимостей нулевого дня, и более того, эти эксплойты были достаточно старыми. Поэтому **даже обычное обновление программного обеспечения не позволяло атакующим попасть в корпоративную сеть**. В некоторых атакованных банках это требование не соблюдалось.

В тех случаях, когда атакующие сталкивались с обновленным программным обеспечением, они отправляли документ

без эксплойтов, но со специальными документами, содержащими макросы, которые должны были загрузить и запустить вредоносную программу.

В этом случае заражение не проходило автоматически и требовало участия сотрудника банка. По умолчанию выполнение таких макросов блокируется самим Word, Excel, PowerPoint и для их выполнения пользователь должен разрешить их выполнение следуя инструкциям злоумышленника.

Чтобы блокировать возможность попадания вредоносной программы таким способом достаточно **установить запрет на выполнение и снятие блокировок макросов с помощью групповых политик для определенных категорий пользователей**. Кроме того, необходимо **оповестить пользователей** о том, что включение макроса может привести к заражению.

Если компьютеры были обновлены и пользователи не следовали инструкциям атакующих, то хакеры отправляли вложения с исполняемым файлом в архиве с паролем. Такие атаки **легко отбить, отправляя подобного рода письма в карантин на проверку**.

ПРЕДОТВРАЩЕНИЕ НА ЭТАПЕ РЕАЛИЗАЦИИ АТАКИ

Даже если злоумышленники получили доступ в корпоративную сеть, атаку можно успешно предотвратить. После того как атакующие попали в сеть банка, им еще предстоит изучить ее, найти интересующие их системы, получить к ним доступ, подготовить схему обналачивания. Все это занимает дни, а иногда месяцы, и это время надо использовать для выявления действий атакующих.

Злоумышленники используют вредоносные программы, которые передают данные на сервер управления. Эти **сетевые взаимодействия между зараженным компьютером и удаленным сервером можно идентифицировать, анализируя сетевой трафик**. Для этого есть готовые решения вроде IDS/IPS и более комплексные системы.

Если у вас нет подобных решений или вы используете решения компаний, которые не отслеживают действия подобных преступных групп, **необходимо использовать данные киберразведки от разных поставщиков и осуществлять проверки по индикаторам**, которые они предоставляют. Индикаторы по группе Buhtrap вы найдете в следующем разделе.

Кроме вредоносных программ атакующие используют **средства удаленного управления, которые можно обнаруживать средствами антивирусной защиты**.

И, пожалуй, самое важное:
если вы обнаружили следы целенаправленной атаки на любом из ее этапов, нужно привлекать профильные компании для ее исследования. Неправильное реагирование приводит к тому, что часть действий атакующих остается незамеченными и злоумышленники добиваются поставленных целей — хищений.

Buhtrap NSIS

http://playback.savefrom.biz/video/video_1.cab
<http://download.sendspace.biz/file/install.cab>
<http://194.58.100.211/install.cab>
<http://download.source-forge.name/file/program.cab>
<http://cams.web-filecab.info/cams/video2.cab>
<http://cache-datamart-windows.com/source/source.cab>
<http://check-mate7.com/kliko/res1.cab>
<http://new.pikabu-story.com/file/file2.cab>
<http://game.sport-box.org/dcim/install.cab>
http://gazprombank.com.ru/dropi/baza_dropov.xls
http://cbr.com.ru/vacansiy/вакансия_No36.zip

Buhtrap C&C

<http://google997.com/info/menu.php>
<http://autopiter.biz/info/menu.php>
<http://google9971.com/info/menu.php>
<http://microsoft7751.com/info/menu.php>
<http://compatexchange-cloudapp.net/help/menu.php>
<http://mp3.ucrazy.org/music/index.php>
<http://uchet.grandars.info/info/menu.php>
<http://ndfl.pravcons.biz/info/menu.php>
<http://rss.sport-express.biz/info/menu.php>
<http://forum.ru-tracker.net/info/menu.php>
<http://microsoft775.com/info/menu.php>
<http://icq.chatovod.info/info/menu.php>
<http://yaf.buhgalter911.biz/topics/menu.php>
<http://forum.zaycev.biz/info/menu.php>
<http://res.buhgalter911.info/info/menu.php>

<http://football.championat.biz/info/menu.php>
<http://tvit.live-journal.info/info/menu.php>
<http://rs-term.org/res1/menu.php>

Почтовые серверы

mail.cbr.ru.com
mail.cbr.ru.net
cbr.ru.com
cbr.com.ru
cbr.ru.net
gazprombank.com.ru
213.159.215.119

LiteManager C&C

forum.buhgalt.net
forum.buhnalog.org
forum.glavbukh.net
tv.hdkinomax.org
rus-gazeta.biz
setting-sandbox-microsoft.com
89.108.101.61
193.124.17.223
37.140.195.165
37.143.12.190
5.63.159.32
194.58.97.249
178.21.10.33
151.248.125.251

Подписчики сервиса киберразведки Bot-Trek Intelligence узнавали о фишинговых письмах Vuhtrap в день их рассылки. Наши консультации помогли жертвам вовремя остановить атаку, полностью очистить сеть и закрыть доступ атакующим.

Мы можем быть полезны на всех этапах атаки. Позвоните или напишите нам, чтобы узнать больше:
[+7 495 984-33-64](tel:+74959843364)
info@group-ib.ru

Threat Intelligence



Киберразведка по подписке — мониторинг, анализ и прогнозирование угроз для компании, ее партнеров и клиентов

TDS



Сенсор для мгновенного выявления зараженных устройств в сети, целевых атак, проникновений и утечек

Центр реагирования CERT-GIB

Круглосуточная помощь опытных специалистов в реагировании на инциденты

Расследования и криминалистика

Безупречный сбор доказательной базы и оперативное установление личностей преступников

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий; первый российский поставщик threat intelligence решений, вошедший в отчеты Gartner.

В 2015 году Group-IB была названа в числе 7 самых влиятельных игроков в сфере информационной безопасности по версии британского издания Business Insider.

Узнайте больше на www.group-ib.ru