SILENCE

Угроза финансовому сектору

ROOT LEVEL RESOURCES

Активное присутствие в XXI веке во всех сферах жизни общества информационных технологий дало мощный толчок развитию кибепреступности в финансовой сфере.

Количество киберпреступлений в России растет из года в год, так как эта сфера преступлений пока еще остается проблематичной для ее предупреждения и оперативной борьбы с ней. Так, согласно данным международной компании Group-IB, которая занимается расследованием и предотвращением киберпреступлений, в среднем в России каждый месяц успешно взламывают 1-2 банка, средний ущерб такого кибероограбления составляет 132 млн. рублей (примерно 2 млн. долларов США).

Опасность киберпреступлений для организаций компаний, работающих в финансовой сфере состоит в том, что цифровые технологии развиваются крайне стремительно и хакеры изобретают новые способы обхода систем безопасности, к которым текущие системы защиты не готовы.

Оценивая рынок высокотехнологичных преступлений в России стоит выделить несколько сегментов, а именно: хищения с помощью троянов для ПК, хищение физических лиц с Android троянами, целевые атаки на банки, фишинг и обналичивание похищаемых средств. Согласно отчету, подготовленного специалистами Group-IB за последние годы, можно выделить следующие этапы развития данных сегментов:

Период: 2017-2018 / 2018-2019

Хищение юридических лиц с троянами для ПК

Показатель	2017-2018	2018-2019
Количество групп	3	2
Общее число успешных атак в день	2	0,5
H2 - H1 (в RUR)	547 800 000	62 250 000
H2 - H1 (в USD)	9 130 000	957 692
Рост к прошлому периоду	-12%	-89%
Средняя сумма одного хищения	1 100 000	500 000
Средняя сумма хищения в день	2 200 000	250 000

Хищение физических лиц с Android троянами

Показатель	2017-2018	2018-2019
Количество групп	8	5
Общее число успешных атак в день	110	40
H2 - H1 (в RUR)	191 730 000	109 560 000
H2 - H1 (в USD)	3 195 500	1 685 538
Рост к прошлому периоду	-77%	-43%
Средняя сумма одного хищения	7 000	11 000
Средняя сумма хищения в день	770 000	440 000

Целевые атаки на банки

Показатель	2017-2018	2018-2019
Количество групп	3	3
Общее число успешных атак в день	-	-
H2 - H1 (в RUR)	1 303 900 000	93 000 000
H2 - H1 (в USD)	21 731 667	1 430 769
Рост к прошлому периоду	-20%	-93%
Средняя сумма одного хищения	118 000 000	31 000 000
Средняя сумма хищения в день	-	-

Фишинг

Показатель	2017-2018	2018-2019
Количество групп	26	11
Общее число успешных атак в день	108	435
H2 - H1 (в RUR)	250 992 000	86 652 000
H2 - H1 (в USD)	4 183 200	1 333 108
Рост к прошлому периоду	6%	-65%
Средняя сумма одного хищения	1 000	800
Средняя сумма хищения в день	1 108 000	348 000

Обналичивание похищаемых средств

Показатель	2017-2018	2018-2019
H2 - H1 (в RUR)	919 543 500	158 157 900
H2 - H1 (в USD)	15 325 725	2 433 198
Рост к прошлому периоду	-34%	-85%
Средняя сумма одного хищения	-	-
Средняя сумма хищения в день	1 336 500	467 100

Из-за динамично развивающихся информационных технологий виды финансовых кибератак видоизменяются, а схемы получения противозаконного заработка с каждым годом становятся все изощреннее. На данный момент можно выделить следующие виды финансово ориентированных кибер-преступлений:

Фишинг

Это один из самых старых и простых видов интернет-мошенничества. Одной из основных причин его популярности является простота его реализации.

Целью фишинга является получение доступа к средствам аутентификации клиента, к конфиденциальным данным пользователей – паролям и логинам учетной записи в системе электронного банкинга. В основном используется метод массовых рассылок от имени известных компаний и организаций, в которых содержатся ссылки на вредоносные сайты, которые внешне не отличить от настоящих;

Программы-вымогатели

Программы, ограничивающие доступ пользователя к электронному устройству и требующие выкуп за возвращения права доступа;

Финансовое мошенничество

Это вид преступных действий, которые осуществляются с помощью информационных систем и направлены на кражу у пользователей конфиденциальных данных и финансовых средств. Ярким примером является почтовое мошенничество, где темами писем являются предложения фальшивых антивирусов, быстрых и высоких заработков, а также сообщения о предварительном одобрении кредитных карт;

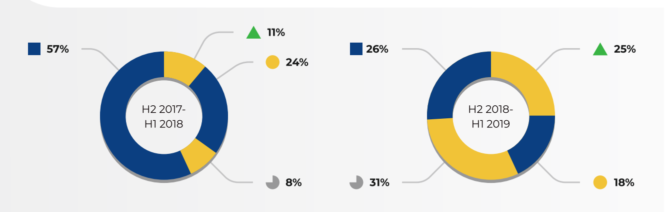
Шпионская программа

Тип вредоносного программного обеспечения, присутствие которого в системе является практически незаметным для пользователей и частично невозможным к обнаружению. Данная программа собирает информацию о поисковых запросах, привычках и предпочтениях пользователя устройства, или же его конфиденциальные данные – например, пароли от банковских аккаунтов или же данные банковской карты, и незаметно для пользователя отправляет их сервера, принадлежащие мошенникам;

Ботнет (сеть ботов)

Это компьютерная сеть, на устройства которой скрытно установлено вредоносное ПО, позволяющее киберпреступникам удаленно управлять вычислительными ресурсами зараженных устройств. Сотни или даже тысячи зараженных таким программным обеспечением устройств используются злоумышленниками для рассылки спама и вирусов, кражи личных данных пользователей и DDoS атак. На сегодняшний день данная угроза является одной из самых серьезных среди киберугроз.

Подводя итоги, рынок высокотехнологичных преступлений в России данных сегментов выглядит следующим образом:



На сегодняшний день, миру известны 5 групп, представляющих реальную угрозу для банков в разных регионах мира, а именно Cobalt; MoneyTaker; Silence; SilentCards; Lazarus. Они используют разные векторы атак, способы проникнуть в изолированные системы и вывести деньги.

Стоит сразу отметиться что Cobalt, MoneyTaker и Silence являются русскоговорящими группами, которые набравшись опыта атак на банки России и СНГ с 2018 года фокусируют свое внимание на иностранных банках и организациях.

Молчание не перекричать.

Одной из самых быстроразвивающихся, малоизученных активных групп является русскоязычная группировка Silence, впервые появившаяся в 2016 году и которые на сегодняшний день являются одними из самых опасных действующих лиц на хакерской сцене.

Так, согласно данным Group-IB, подтвержденная сума хищений группой Silence с июня 2016 года по 2019 год составила не менее 272 млн. рублей (примерно 4,2 млн. долларов США).

О том что группировка Silence явлвется русскоговорящей свидетельствует то, что команды трояна являються русские слова, набранные на английской раскладке, к примеру: 1) htrjyytrn = reconnect = реконнект, 2) htcnfhn = restart = рестарт, 3) ytnpflfx = notasks = нетзадач.

Кроме того, арендованные Silence серверы для осуществления фишинговых атак находятся в России и Нидерландах у русскоговорящих хостеров. Под командные центры они используют услуги хостинга с Украины, который позволяет размещение практически любого контента, в том числе запрещенной информации, вредоносных приложений и файлов.

В мае 2019 года, во время «потрошения» банкомата Dutch-Bangla в Дакке (Бангладеш), камерами видеонаблюдения было зафиксировано видео с обналичиванием денег, на котором было хорошо видно лица преступников.

География атак

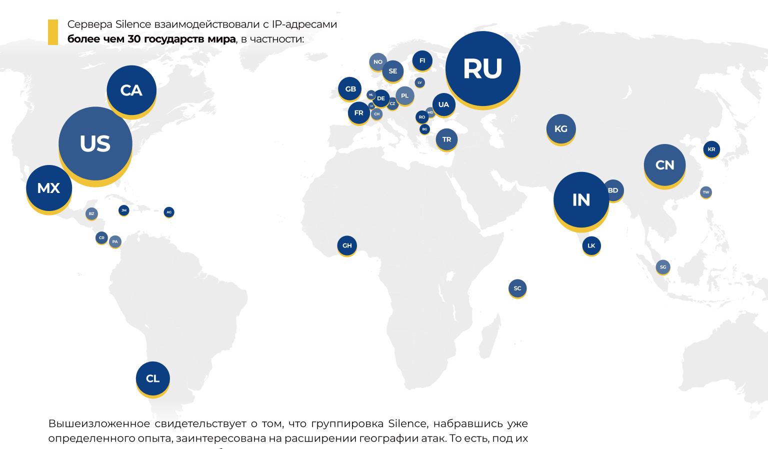
ROOT LEVEL RESOURCES

Таймлайн атак «от России до Латинской Америки»:[1]

Дата	Атака	Результат
Июль 2016	Попытка вывода денег через российскую систему межбанковских переводов АРМ КБР.	**Неудача** Атака сорвалась из-за неправильной подготовки платежного поручения. В банке остановили подозрительную транзакцию и провели реагирование собственными силами.
Август 2016	Silence восстановили доступ к серверам того же банка и предприняли повторную попытку взлома. Для этого они загрузили программу для скрытого создания скриншотов экрана пользователя и начали изучать работу операторов по псевдо-видеопотоку.	**Неудача** Атака была предвращена
Октябрь 2017	Первая атака Silence на банкоматы.	**Успех** За одну ночь они смогли похитить 7 млн рублей.
Февраль 2018	Атака через карточный процессинг.	**Успех** За выходные Silence удалось снять с карточек через банкоматы 35 млн рублей
Апрель 2018	Новая атака Silence через банкоматы.	**Успех** За одну ночь им удалось похитить 10 млн рублей
Май 2018	Массовая отправка вредоносных писем на русском языке в котором находился эксплоит, с помощью которого загружалось вредоносное ПО.	**Неизвестно**
Август 2018	Атака на банк Индии.	**Успех**
Октябрь 2018	Вредоносная рассылка по российским банкам.	**Неизвестно**
	Тестовая рассылка по британским финансовым компаниям.	**Неизвестно**
Ноябрь 2018	Массовая фишинговая рассылка от имени Центробанка РФ.	**Неизвестно**
	Тестовая рассылка в азиатскую компанию.	**Неизвестно**
Декабрь 2018	Вредоносная рассылка.	**Неизвестно**
Январь 2019	Атака по финансовым компаниям Великобритании.	**Неизвестно**
Февраль 2019	Новая атака на банк Индии.	**Неизвестно**
	Атака на Омский «ИТ Банк» в России.	**Успех** Вывод средств в размере 25 млн рублей
Май 2019	Атака банка Dutch-Bangla в Бангладеше.	**Успех** Украдено около 3 млн долларов США
Июль 2019	Атаки на банки в России, Гане, Болгарии, Чили, Коста-Рике.	**Успех**

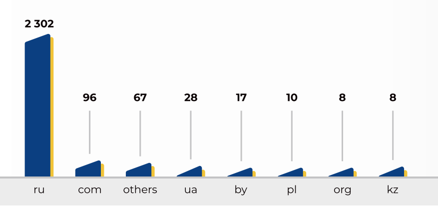
[1] *Преступления раскрытые экспертами Group-IB*

Сервера Silence взаимодействовали с IP-адресами **более чем 30 государств мира**, в частности:



Вышеизложенное свидетельствует о том, что группировка Silence, набравшись уже определенного опыта, заинтересована на расширении географии атак. То есть, под их прицелом может оказаться любое государство.

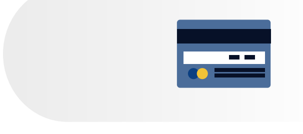
Статистика результатов взаимодействия с IP-адресами выглядит следующим образом:



Кроме того, стоит отметить, что эксперты Group-IB заявили, что Silence уже начала приобретать установки своего трояна в банки через хакерскую группу – TA505. Коллаборации с другими хакерскими группировками, вероятно, также приведет к тому, что география атак будет сильно расширена.

Векторы атак Silence

ROOT LEVEL RESOURCES



1. Карточный процессинг – как основной способ хищения

Атаки на карточный процессинг по-прежнему являются одним из основных способов хищений и проводятся группами Cobalt, MoneyTaker, Silence. Этот метод обеспечивает самый безопасный способ обналичивания и максимальную финансовую выгоду. С марта 2018 года самые успешные атаки на банкоматы принадлежат Silence (в 2016, 2017 году лидерами были Cobalt).

Данный способ хищения состоит из нескольких этапов атаки:

1. Получение контроля над банковской сетью
2. Проверка возможности подключаться к системе управления карточным процессингом
3. Открытие или покупка карт банка, к которому был получен доступ
4. Подготовка мулов, которые с этими картами выезжают в другую страну
5. Отключение или увеличение лимита на снятие наличных для этих карт
6. Отключение овердрафт-лимитов, чтобы можно было уйти в минус даже по дебетовым картам;
7. Снятие наличных мулами по команде в разных банкоматах

Для таких операций группа обычно использует собственный троян Atmosphere. На протяжении видимой деятельности группы троян модифицировался, чтобы соответствовать требованиям атакующих. Так, троян изменил логику внедрения в процессы с помощью гибкого инжектора, что позволило расширить перечень поддерживаемых банкоматов. Постепенно из троян убирали ненужных функций, которые мешали или не использовались при атаках.

2. ATM-троян (xfs-disp.exe)

В феврале 2019 года было обнаружено, что Silence начала проводить успешные атаки с помощью нового трояна, в коде которого содержатся признаки того, что она нацелена на хищение валюты в долларах. Данный троян позволяет получать информацию о разных устройствах банкомата и выводить ее администратору либо в окно на экране; подменять данные о кассетам АТМ, а также выводить наличные из банкоматов.

3.Атаки на автоматизированное рабочее место клиента Банка России (АРМ КБР)

В 2016 году основную угрозу для банков в России представляли атаки на АРМ КБР. Однако, с 2017 года Silence игнорирует данные системы даже в том случае, когда успешно получают к ним доступ. Сейчас их внимание привлекают более надежные схемы хищений через банкоматы и карточный процессинг.

Оружие Silence для сражений в киберпространстве.

ROOT LEVEL RESOURCES

Следует сразу отметить, что главным инструментов хакера-профессионала является мозг. Именно с помощью интеллекта и знаний хакер способен создавать и эффективно приманять виртуальное оружие для сражений в киберпространстве. Таким виртуальным оружием являються специальные програмные инструменты, индивидуальные для каждого сценария атаки.

Исследования лаборатории криминалистики Group-IB показали, что в начале своего пути Silence использовали чужие инструменты, такие как Smoke bot (бот для проведения первой стадии заражения) и модифицированный Perl IRC DDoS bot, основанный на Undernet DDos bot, для осуществления DDos-атак. Silence учились буквально по ходу атаки.

Однако очень быстро они начали создавать собственное виртуальное оружие, в результате чего усовершенствовали тактику в киберпространстве. Так, преступники разработали свой уникальный набор инструментов для кибератак, включающий в себя самописные программы:

Silence Trojan

Один из основных инструментов группы — одноименный уникальный модульный фреймворк, созданный для атаки на инфраструктуру, который состоит из следующих компонентов:

1) Загрузчик Silence.Downloader;
2) Основной модуль Silence и пропатченный бэкдор Kikothac;
3) Модуль слежки за пользователем Silence.SurviillanceModule;
4) Proxy Silence Proxybot.

Этот троян и его модули слежки используются для установки канала святи между изолированными сегментами корпоративной сети жертвы и управляючим сервером преступников.

Silence Proxybot

Уникальная программа, которая позволяет перенаправлять трафик между удаленным и локальным сервером, может собирать и отправлять на удаленный сервер информацию о системе, сохранять данные в реєстр.

Atmosphere

Уникальный набор программ для «потрошения» банкоматов, который содержит программу для работы с диспансером и программу для внедрения вредоносной библиотеки в процесс диспансера.

Xfs-disp.exe

Троян для атаки на банкоматы. Программа позволяет получать информацию о разных устройствах банкомата и выводить ее администратору либо в окно на экране; подменять данные о кассетам АТМ, а также выводить наличные из банкоматов.

Ivoke

Первый бесфайловый модуль (троян) с целью получения сведений о зараженной системе и загрузки следуоей стадии по команде от управляющего сервера.

Cleaner

Инструмент для записи мукора в файл логов подкобчения к серверу, развернутому на атакуемой машине, и для дальнейшего удаления файла.

Farse

Утилита для извлечения учетных данных пользователей и системы (получения паролей с зараженного компьютера)

EDA-EmpireDNSAgen (empire+dnscat2)

Используется для управлния скомпрометированной системой и позволяет командной оболочке выполнять задачи, туннелировать трафик, используя про этом протокол DNS.

PowerMTA

Широкоизвестное програмное обеспечение, используемое для рассылки почты

Metaspoit

Широкоизвестный фреймворк с продуманной архитектурой, сотнями контрибьюторов, который включает в себя тысячи модулей для авторизации эксплуатации огромного количества уязвимостей.

Mimikatz

Широкоизвестная утилита, которая позволяет извлечь аутентификационные данные залогинившегося в системе, а также использовать их для взлома других доступных устройств.

Winexe

Широкоизвестная программа (файл), который способен изменить настройки комп'ютера и нанести ему вред.

Radmin

Широкоизвестная программа удаленного администрирования ПК для платформы Windows, которая позволяет полноценно работать на нескольких удаленных компьютерах с помощью графического интерфейса, а также позволяет передавать файлы и использовать режим голосового или текстового общения с пользователем удаленного компьютера.

Стоит отметить, что в связи со стремительным развитием информационных технологий и кибербезопасности, кибепреступникам приходится постоянно создавать новые и модифицировать свои инструменты для сражений в киберпространстве, чтобы успешно обходить системы информационной безопасности. Поэтому провайдерам сетевой безопасности, как говорится «покой только снится».

Каждое слово имеет последствия. Каждое молчание, тоже.

Подводя итоги, следует отметить, что ситуация с киберпреступлениями в России двоякая: с одной стороны, наблюдается увеличение количества преступлений с использованием информационных технологий, с другой – снижается объем хищений в финансовой сфере. Опасность данной угрозы становится все более очевидной, и кредитно-финансовые организации, и государство в целом проводят различные мероприятия для уменьшения риска стать жертвами киберпреступлений. В данный момент киберпреступления опасны тем, что преступники осуществляют свои действия дистанционно, а также способны за короткий срок с момента начала преступления украсть огромные суммы денег.

Какова же реальная цена, которую платит жертва кибератаки?

Весьма очевидной ценной являются потеря данных и средств; штрафы, налагаемые регулирующими органами; издержки, связанные с общественным резонансом; расходы на уведомление о происшествиях и усиление мер защиты. Однако не стоит упускать тот факт, что последствия кибератаки могут напоминать о себе на протяжении многих лет, выливаясь в целый ряд скрытых издержек, в частности:

- Ущерб репутации;
- Сбои в работе;
- Утраты конфиденциальной информации и прочих активов стратегического значения;
- Судебные тяжбы и прочее.

Не всегда учитываются и редко когда становится известны общественности и поддаются анализу последствия, которые носят нематериальный характер, а именно:

- Ущерб торговых марок;
- Утрата интеллектуальной собственности;
- Расходы, связанные со сбоями в работе.

Законодательство России в сфере кибербезопасности оставляет желать лучшего. Именно это является одним из главных «стопов» для активной работы мировых лидеров киберстрахования в России. Ведь при урегулировании страховых случаев нужно будет опираться на актуальную законодательную базу и судебную практику. Законом о страховании в Российской Федерации установлено, что страховым случаем является событие, предусмотренное договором страхования или законом, с наступлением которого возникает обязанность страховщика произвести выплату компании, которая приобрела полис, или выгодоприобретателю, или иным третьим лицам. Важным элементом для определения объема ответственности являются условия договора, который заключается между сторонами. Поэтому, мы настоятельно рекомендуем Вам перед подписанием договора привлекать компетентного и независимого специалиста соответствующего профиля (юриста).

Помните, именно от условий подписанного договора будет зависеть объем Вашей ответственности.

Используемые источники:

ROOT LEVEL RESOURCES

1 https://www.youtube.com/watch?v=un1H-92AUeI
2 https://www.thedailystar.net/frontpage/news/three-banks-hit-cyberattacks-1760629
3 https://www.prothomalo.com/economy/article/1597491/%25E0%25A6%25A6%25E0%25A7%2587%25E0%25A6%25B6%25E0%25A7%2587-%25E0%25A6%258F%25E0%25A6%25AE%25E0%25A6%25A8-%25E0%25A6%259C%25E0%25A6%25BE%25E0%25A6%25B2%25E0%25A6%25BF%25E0%25A7%259F%25E0%25A6%25BE%25E0%25A6%25A4%25E0%25A6%25BF-%25E0%25A6%2595%25E0%25A6%2596%25E0%25A6%25A8%25E0%25A7%258B-%25E0%25A6%25A6%25E0%25A7%2587%25E0%25A6%2596%25E0%25A6%25BE-%25E0%25A6%25AF%25E0%25A6%25BE%25E0%25A7%259F%25E0%25A6%25A8%25E0%25A6%25BF&sa=D&ust=1564743784434000&usg=AFQjCNEkBE7L26omHjGM7NuAnSFO2STrMA
4 https://www.dhakatribune.com/error
5 https://www.thedailystar.net/frontpage/news/three-banks-hit-cyberattacks-1760629&sa=D&ust=1564743784434000&usg=AFQjCNFOB7KqwoX53kORZTWb5zM6OC0Xcg
6 https://www.kommersant.ru/doc/3881484
7 Отчеты экспертов Group-IB 2016-2019 // URL: https://www.group-ib.ru/
8 Отчеты центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка Росии // URL: http://www.cbr.ru/
9 Отчеты центра безопасности Symantec // URL: https://www.symantec.com/