# Исследование и анализ вредоносного программного обеспечения Carbanak

Аннотация: в ходе исследования рассмотрены основные признаки, атрибуты и работа вредоносного программного обеспечения Carbonak. В данной работе будет рассмотрена одна из многочисленных целевых атак киберпреступников, а именно нападение на филиал банка с помощью эксплуатации бэкдора Carbanak.

Ключевые слова: Carbanak, вредоносное программное обеспечение, банки, кибербезопасность.

Банковские трояны, ворующие деньги со счетов компаний и простых пользователей, ежегодно наносят ущерб на миллионы долларов. Естественно, вирмейкеры стараются держать все, что связано с внутренней кухней банкеров, в глубочайшей тайне. Обеспечение экономической безопасности страны тесно связано с системой экономической безопасности предприятий, в частности, системой кибербезопасности. По данным обзора компании EY проблема кибербезопасности вышла по значимости на первое место для многих компаний. По одной из оценок в 2019 году преступность в киберпространстве может стоить бизнесу порядка 2 трлн $ (по России).

Сферой деятельности рассматриваемого объекта является денежное обращение предприятия. Функционирование осуществляется, в основном, в сфере производства и обмена. В новом филиале кредитного отдела банка работает 14 сотрудников. (рис. 1)

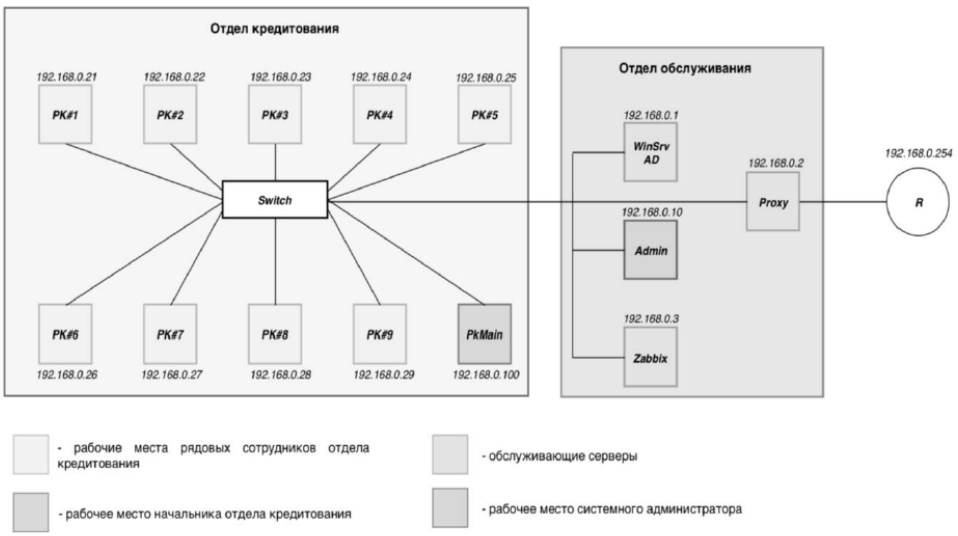


Рисунок 1 – Топология сети

Из рисунка видно, что существует 2 отдела: отдел обслуживания и отдел кредитования. Отдел информационной безопасности в данном примере отсутствует. Его функции исполняет системный администратор:

1. Обнаружение сетевых узлов, открытых портов, которые могли бы идентифицировать ОС и версии серверных приложений.

2. Обновление компонентов системы.

3. Управление доступом в сети.

4. Разработка и внедрение политики безопасности.

5. Анализ и выявление угроз защищаемой информации, причин, условий их возникновения и др.

Первый шаг злоумышленников в целенаправленной атаке - сбор информации о компании, среди которой присутствовали сведения о электронной почте сотрудников.

Далее, на полученные e-mail адреса осуществлялась фишинговая рассылка с вложенным вредоносным программным обеспечением. Один из сотрудников, а именно Столяков Петр Иванович (рабочий отдела кредитования, РК№2, IP-адрес 192.168.0.22), запустил подозрительный файл на своем рабочем месте. Благодаря этому, мошенниками был получен доступ в локальную сеть организации.

Следующим шагом злоумышленников был сбор данных о внутренней инфраструктуре: как устроена работа, функционал и обязанности сотрудников. При помощи зараженного рабочего места было получено управление над всеми хостами локальной сети организации. На данном шаге киберпреступники выяснили, что среди сотрудников отдела кредитования есть начальник, который лично должен подтвердить каждую из направленных транзакций (пополнение счета, перевод денежных средств). Завершающий шаг - хищение денежных средств путем перевода на подставные счета. Данное мероприятие оказалось реализуемым, так как был получен доступ к рабочим местам и сотрудника (посылается заявка), и начальника отдела кредитования (подтверждение транзакции).

После многочисленных переводов денежных средств на счета преступников главный офис банка заблокировал доступ кредитного филиала к базе данных. На место преступления был направлен специалист информационной безопасности, целью которого было расследование инцидента, а также возможная ликвидация его последствий. Так как главный офис банка

ограничил возможности кредитного филиала, то полноценное функционирование оказалось невозможным. Следовательно, было принято решение об отключении филиала от глобальной сети. Таким образом, преступники не смогут удаленно выполнять произвольные команды на зараженных устройствах. В ходе расследования на всех рабочих хостах сети под управлением операционной системы семейства Windows было выявлено наличие файла svchost.exe по пути Windows\System32\com. При детальном изучении запущенных процессов было обнаружено ряд служб, дублирующих службы, которые оканчиваются на «sys», в частности, «aspnetsys» при легитимной службе «aspnet». По словам компании «Лаборатория Касперского», обнаруженные следы свидетельствуют о заражении вредоносным программным обеспечением Carbanak.

Программное обеспечение Carbanak и его модификации имеют следующие hash-суммы: (рис. 2)

1. *3552338D471B7A406D8F7E264E93B848075235C0.*
2. *3A9A23C01393A4046A5F38FDBAC371D5D4A282F1.*
3. *8D5F2BF805A9047D5830978A3C9E8DE395469A8.*
4. *BCF9E4DCE910E9473972815 8C98578A8D145BE56.*
5. *8330BC5A3DCC52A22E50187080A60D6DBF23E7E6.*
6. *E838004A216E58C44553A168760100B497E514E8.*
7. *CF1F97879A6EB26FEDC7207D6679DFA221DD2D45.*
8. *72677913402040207279 23CC7C8D65AFC18F6F5B.*
9. *F8CBF647A64028CAE835A750EF3F8D1AA216E46C.*
10. *33870482BA7DE041587D4B809574B458C0673E94.*
11. *3927835C620058EFCADF76642489FC13AACE305B.*
12. *D678BD90257CF859C055A82B4A082F9182EB3437.*
13. *0B8605D0293D04BBF61010303976 8CBE62E2FAAE.*
14. *7A9BE31078BC9B5FECE94BC1A9F45B7DBF0FCE12.*

Рис. 2

Сертификат которым был подписан вредоносный файл: (рисунок 3)

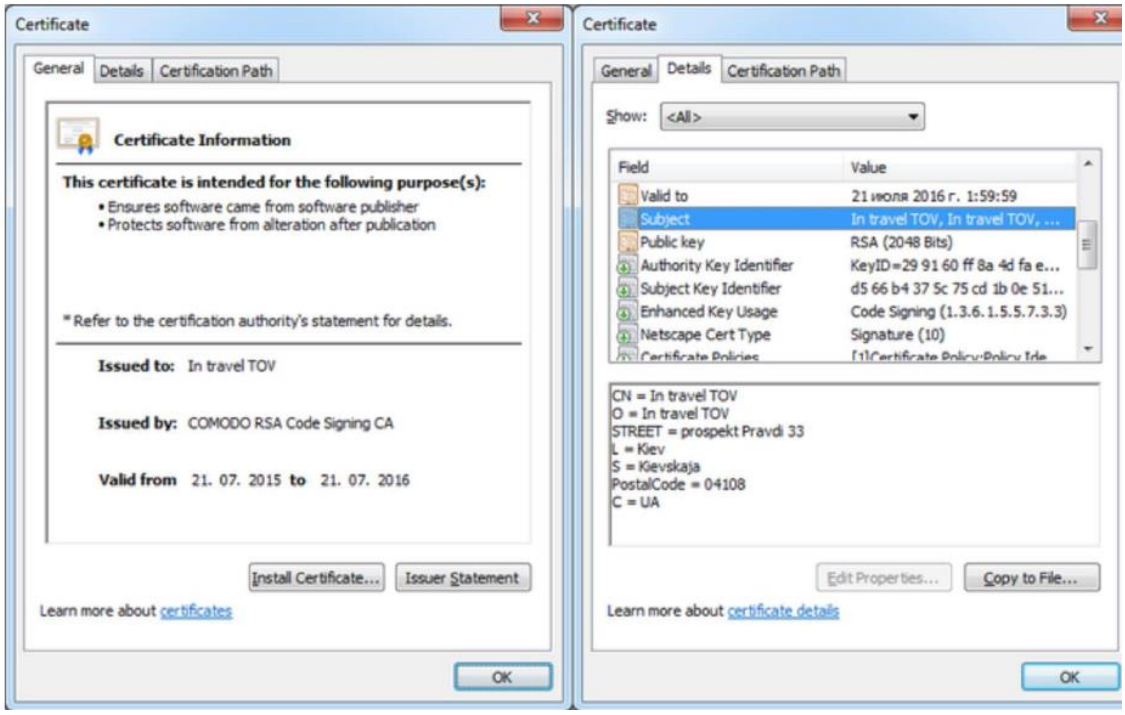


**Рис. 3**

Основные положения, свойственные для перехваченного сертификата: (рис.4)

1. **Company name:** *In travel TOV.*
2. **Validity:** *from 21 July 2015 to 21 July 2016.*
3. **Thumbprint:** *7809fbd8d24949124283b9ff14d12da497d9c724.*
4. **Serial number:** *00dfd915e32c5f3181a0cdf0aff50f8052.*
5. **Subject:** *CN = In travel TOV.*
6. **O** = *In travel TOV.*
7. **STREET** = *prospekt Pravdi 33.*
8. **L** = *Kiev.*
9. **S** = *Kievskaja.*
10. **PostalCode** = *04108.*
11. **C** = *UA.*

(Рис. 4)

С целью предотвращения заражения вредоносным программным обеспечением Carbanak, специалистами информационной безопасности были предложены следующие рекомендации:

1. Проведение обучающих занятий в сфере ИБ с сотрудниками компаний.

2. Воздержание от открытия подозрительных электронных писем.

3. Установка антивирусного программного обеспечения на узлы сети.

4. Внедрение систем обнаружения вторжений (IDS/IPS).

5. Настройка межсетевого экрана.

6. Ограничение учетных записей.

7. Сегментирование сети по отделам.

8. Использование SIEM-систем для централизованного мониторинга.

9. Регулярное обновление программного обеспечения.

Список литературы


1. АНАЛИЗ С ДАЛЬНЕЙШИМ МОДЕЛИРОВАНИЕМ ПОВЕДЕНИЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS NT ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ CARBANAK [Электронный источник] – URL: https://elibrary.ru/
2. МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ CARBANAK [Электронный источник] – URL: https://elibrary.ru/
3. МОДЕЛИРОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОМОЩИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ CARBANAK [Электронный источник] – URL: https://elibrary.ru/
4. CARBANAK APT THE GREAT BANK ROBBERY [Электронный источник] – URL: https://www.kaspersky.com/