МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01ммзи
_____ Цой Ю.Р.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику **3**

Введение **4**

Атаки на банкоматы **5**

Основные типы атак 6

Атака на АТМ с помощью Carbonak **7**

Вывод 5

Заключение **15**

Список используемых источников 16

Задание на практику

- Исследование атак на АТМ

- Исследование вредоносного программного обеспечения Carbanak

- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с вредоносным программным обеспечением для атак на банкоматы.
2. Теоретически ознакомиться с методами взлома и изучить принципы взлома банкоматов.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Атаки на банкоматы

Аннотация:

Данная статья посвящена рассмотрению проблемы взлома банкоматов и наиболее распространённым видам атак. В статье выявлены основные методы, используемые злоумышленниками; средства, предназначенные для взлома банкоматов; общий алгоритм действий хакера при использовании конкретных типов защиты. В заключении подведен итог по поводу действенности материала, указанного в статье.

Предисловие

В последние годы, одновременно с развитием банкоматной сети, выросло и количество случаев банкоматного мошенничества. Злоумышленники используют взлом как средство кражи денежных средств. И несмотря на то, что банкоматы имеют достаточно серьезную защиту, в настоящее время существует множество методов атаки на них. В данной статье мною будут рассмотрены методы атаки на банкоматы с целью хищения денежных средств, как с пластиковых карт, так и непосредственно из самих банкоматов.

Перед тем как узнать методы атаки и способы защиты от них, нужно иметь общее представление о функционировании банкоматов. Сам банкомат (или ATM – Automated Teller Machine) представляет собой компьютер, совмещенный с сейфом. Компьютер, как правило, оснащен устройством ввода, дисплеем, кардридером (для чтения данных с пластиковой карты), презентером (для выдачи кэша), чековым/журнальным принтеромиди диспенсером – девайсом, предназначенным для взятия/подачи денежных купюр, их проверки на подлинность и сортировки.

Основные типы атак на ATM

1. Одним из самых распространенных способов физического доступа к карте является установка скиммера в банкомат. Скиммер (от «skim» – снимать сливки) – специальное считывающее устройство, работающее прослойкой между картой и банкоматом. Данное устройство присоединяется к лотку приёма карт в банкомате и пропускает карты сквозь себя, чтобы считать информацию специальной головкой. Считыватель может дополняться мобильной камерой, записывающим PIN, вводимым пользователем на клавиатуре, а также специальной накладной клавиатурой, которая запоминает введённую вами последовательность. Такие устройства работают от батареек, однако, чаще всего не передают информацию по сети: злоумышленнику нужно будет снять их с банкомата и подключить к компьютеру, для получения собранных данных.

2. Другое устройство – lebaneseloop (ливанская петля). Оно представляет собой пластиковый конверт, размер которого немного больше размера карточки – его закладывают в щель банкомата. Банкомат не может прочитать данные с магнитной полосы. Владелец карты пытается ее вернуть, но из-за конструкции конверта этого сделать не получится. В это время подходит сам злоумышленник, говорит, что с ним случилась та же самая ситуация и рассказывает как вернуть карту. Владелец карточки пробует, но ничего не получается. Он думает, что его карточка осталась в банкомате и уходит для того, чтобы связаться с банком. Мошеннику только и остается, что достать конверт вместе с кредитной картой при помощи подручных средств и снять деньги со счета.

3. Технически сложный способ. Можно перехватить данные, отправляемые банкоматом в банк для того, чтобы удостовериться в наличии запрашиваемой суммы денег на счету. Мошенникам необходимо подключиться к соответствующему кабелю и считать необходимые данные.

4. Дорогостоящий, но действенный способ – мошенники ставят в людном месте свой собственный «банкомат». На самом деле, он не работает и, естественно, никаких денег не выдает. Однако в свою очередь он успешно считывает с карточки владельца все необходимые данные. Несколько советов как защитить свою карту от мошенников:

5. Другим методом взлома банкомата является кража денежных средств при помощи вредоносных программ (Carbonak).

Атака на АТМ с помощью Carbonak

Полностью процедура от заражения первого компьютера и до сокрытия следов преступления занимала в среднем от двух до четырех месяцев на один банк. Особенность ограбления состояла в том, что хакеры не зависели от используемого банком программного обеспечения, даже если у банка оно было уникальным. Преступники не взламывали банковские сервисы, они проникали в корпоративную сеть и тем самым все их действия не вызывали подозрений. Киберпреступники попадали в банковскую сеть через электронные письма, которые рассылались сотням банковских служащих, которые заведомо содержали в себе вирус «Carbanak». После того как был заражён один из компьютеров, хакеры находили компьютеры администраторов систем денежных транзакций и разворачивали видеонаблюдение за их экранами.

Процесс кражи денег группировкой «Carbanak» проходил следующим образом.

1. Для снятия денег киберпреступники использовали онлайн-банкинг или платёжные системы для перевода денежных средств со счета банка на свои счета, которые были открыты в банках Китая и Америки.

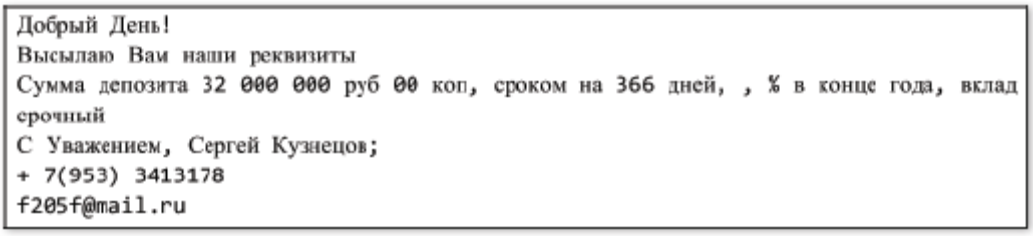
2. Выявлены случаи, когда хакеры проникали в систему бухгалтерского учёта и при помощи мошеннических транзакций «раздували» баланс средств на счете, то есть киберпреступники узнавали, что на счете находится 3 тысячи дол., тогда они увеличивали баланс до 10 тысяч и переводили 7 тысяч себе. Владелец счета ничего не узнавал о данных транзакциях, поскольку деньги его оставались на месте.

3. Помимо всего прочего, киберграбители получали контроль над банкоматами и активировали команды на выдачу наличных в установленное время. После этого к банкомату подходил кто-нибудь из членов банды и забирал деньги. Переходя непосредственно к вопросу об угрозе внутреннего инфицирования банковских компьютеров вредоносным программным обеспечением, стоит отметить случай обнаружения уникального вируса. Хакерская профессиональная группа «EquationGroup», ведет свою деятельность на протяжении почти двадцати лет, и ее действия затронули тысячи, а возможно, и десятки тысяч пользователей в более чем 30 странах мира. Наиболее пострадавшими называются Иран, Россия, Пакистан, Афганистан, Китай, Мали, Сирия, Йемен и Алжир

Техническая реализация Carbonak

Первоначальные инфекции достигались с помощью целевых фишинговых писем, с прикрепленными файлами Microsoft Word 97 - 2003 (.doc), Control Panel Applet (.CPL)

Пример письма:

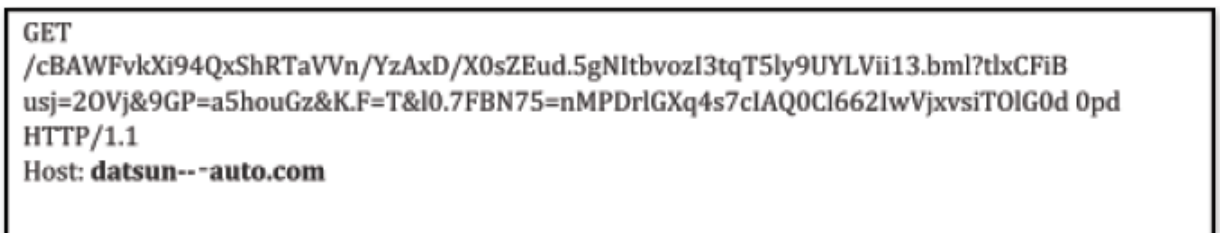


Carbanak - это бэкдор, используемый злоумышленниками для компрометации машины жертвы. После успешного проникновения, Carbanak копирует себя в «% system32% \ com» с именем «svchost.exe» с атрибутами файла: системный, скрытый и доступный только для чтения. Чтобы гарантировать, что Carbanak имеет права на автозапуск, вредоносная программа создает новую службу. Синтаксис именования - «<ServiceName> Sys», где ServiceName – любое существующая служба выбирается случайным образом, с удалением первого символа.

Подключение к заражённому компьютеру происходит с помощью удаленного рабочего стола Протокол (RDP), Carbanak устанавливает режим выполнения службы Termservice на Auto. Также, после выполнения этой службы он изменяет исполняемый код в памяти, чтобы установить одновременные рабочие процессы как для удаленных, так и для локальных пользователей. Модули измененными в этом процессе являются: termsrv.dll, csrsrv.dll, msgina.dll и winlogon.exe.

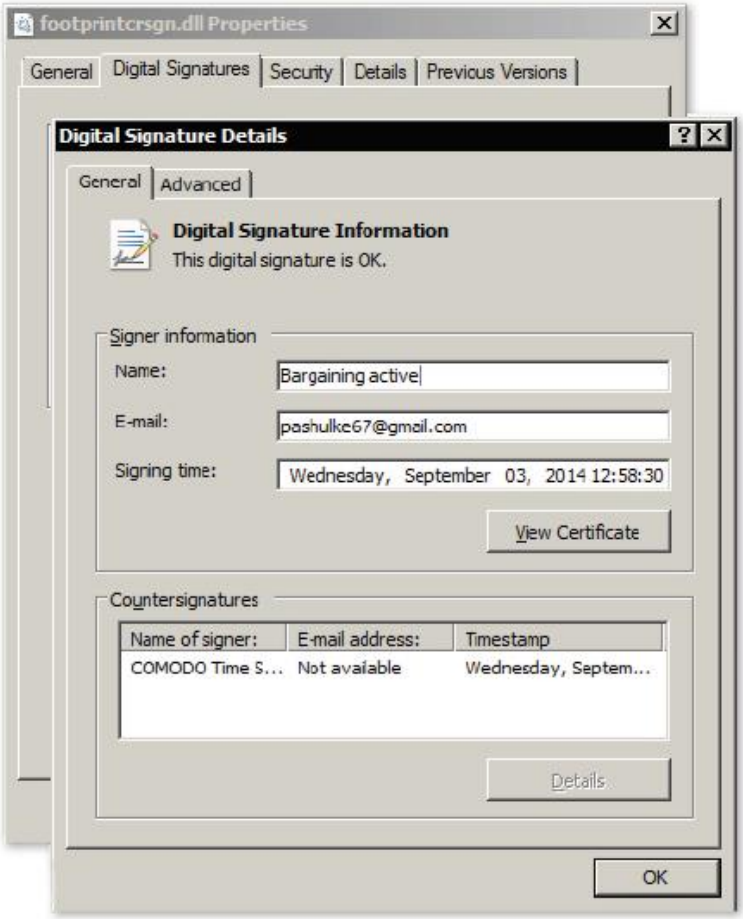
Если Carbanak обнаружит банковское приложение BLIZKO (программное обеспечение для перевода средств) в зараженный компьютер, он отправляет специальное уведомление на свой C2-сервер. Carbanak также знает о банковском приложении IFOBS и может по команде заменить реквизиты платежных документов в системе IFOBS. Для связи со своим сервером C2 Carbanak использует протокол HTTP с Шифрование RC2 + Base64 и добавление дополнительных символов, не включенных в Base64. Он также вставляет строки с разными расширениями (.gif, .htm и т. Д.) В случайные места. в HTTP-запросе.

Пример запроса:



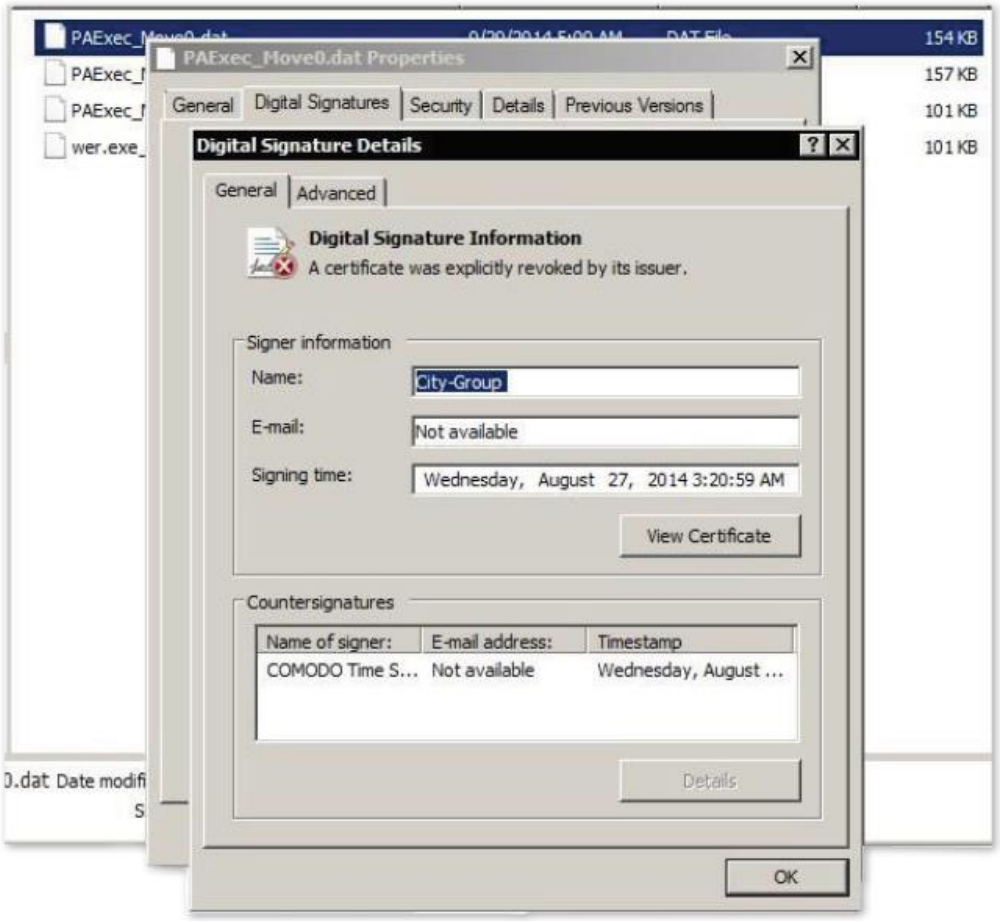
Чтобы сделать вредоносное ПО менее подозрительным, последние образцы Carbanak имеют цифровую подпись:

MD5 08F83D98B18D3DFF16C35A20E24ED49A



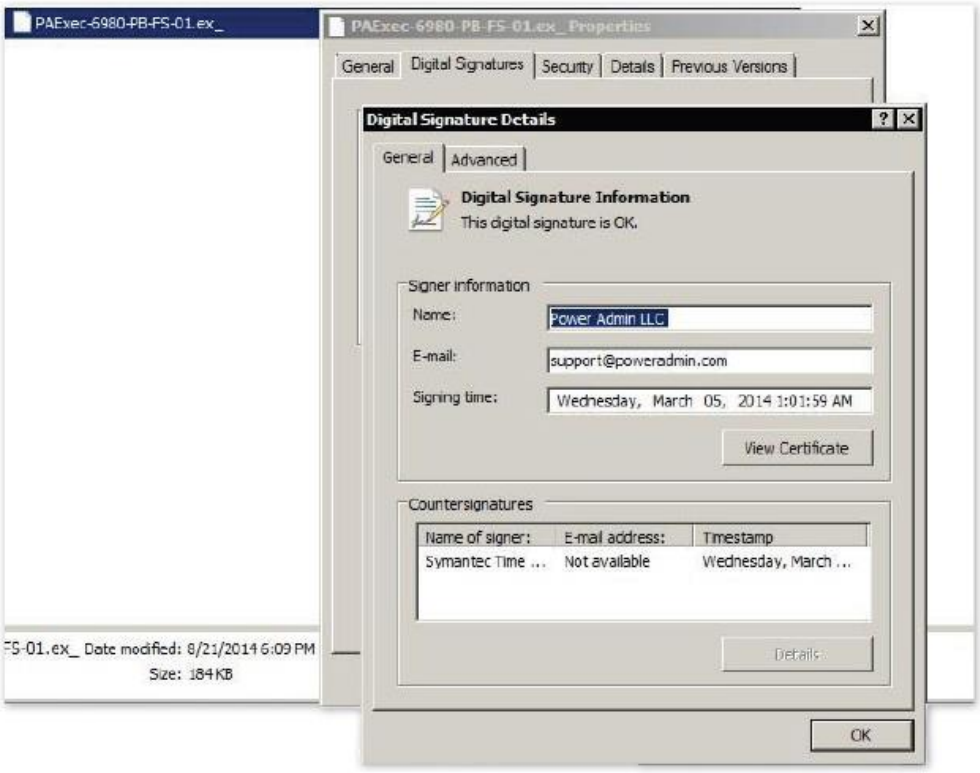
PAExec_Move0.dat

MD5 972092CBE7791D27FC9FF6E9ACC12CC3



Один из инструментов бокового перемещения Carbanak также имеет цифровую подпись:
PAExec-6980-PB-FS-01.ex_

MD5 86A5C466947A6A84554843D852478248



Для Carbonak существует 4 вида серверов

Серверы Linux, используемые для выдачи команд развернутым экземплярам Carbanak.

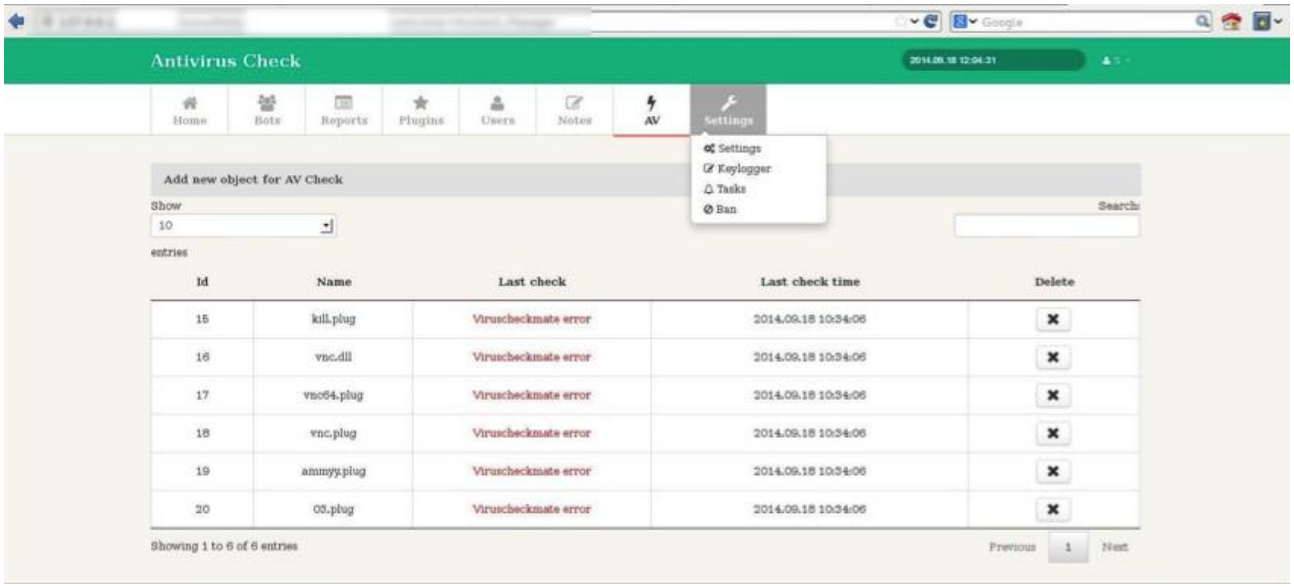
и для получения собранных данных мониторинга;

Серверы Windows, используемые для удаленного подключения к системам-жертвам;

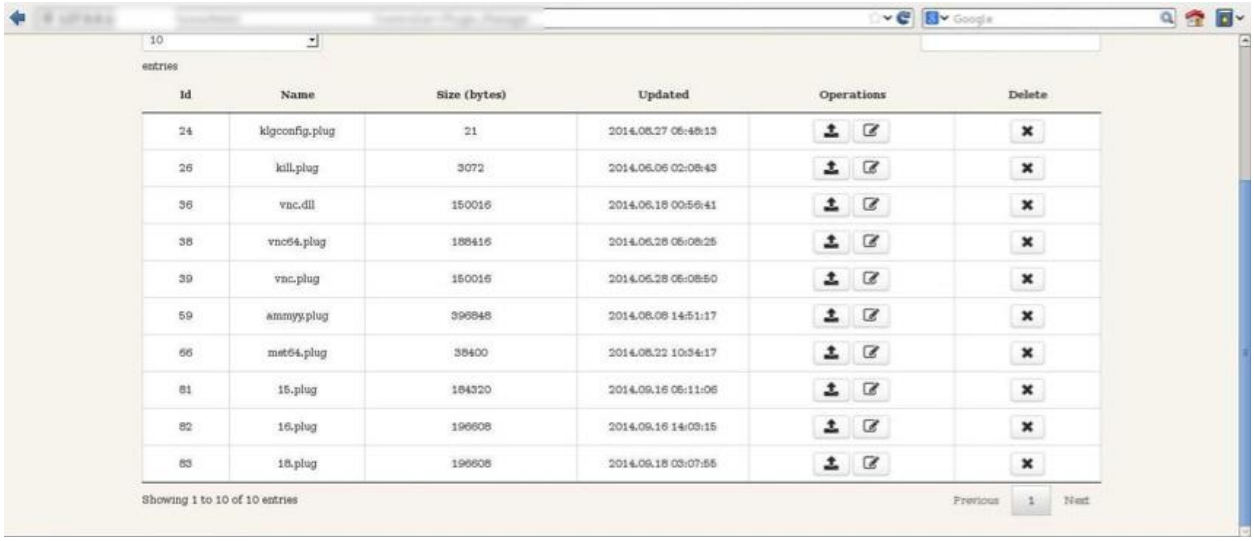
Серверы резервного копирования;

Дроп серверы, на которых находятся дополнительные исполняемые файлы (например, удаленное администрирование

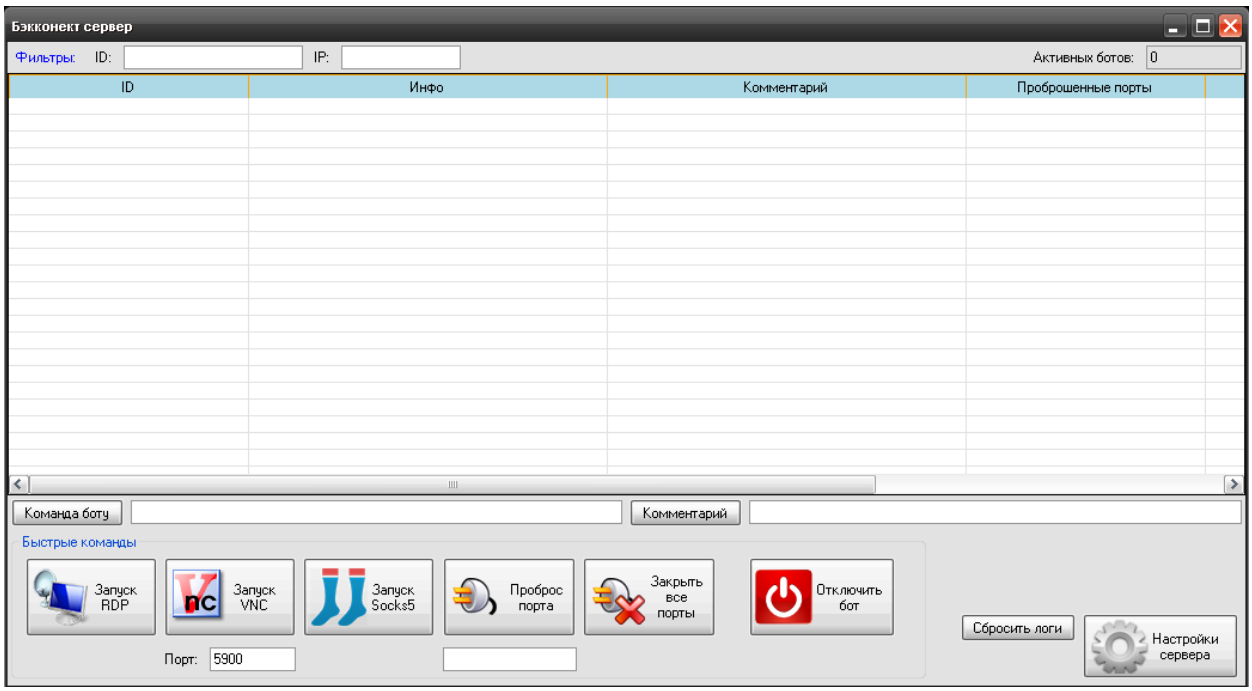
инструменты) размещены.



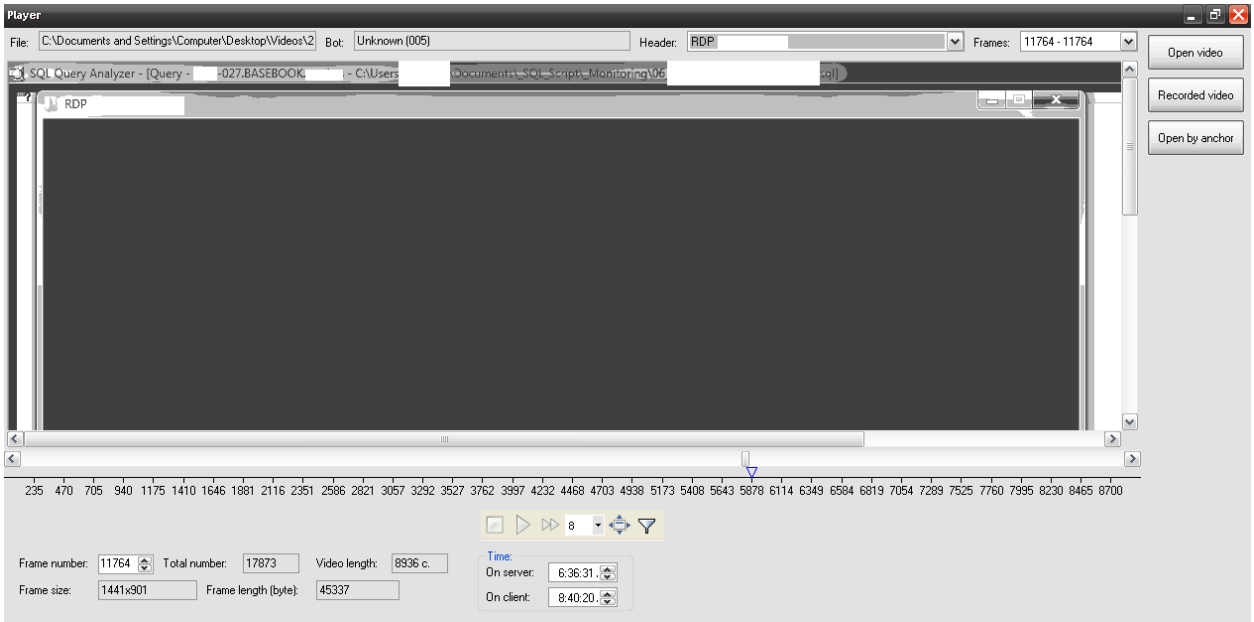
Панель администрирования Carbanak, работающая в Linux



Панель администрирования Carbanak в Linux, список плагинов



Панель администрирования Carbanak, работающая в Windows, может запускать RDP, VNC, прокси и туннели через Carbanak. Системы жертв занесены в каталог в базах данных серверов. Жертвы принадлежат для ряда различных сообществ, что упрощает администрирование. В целом, Было обнаружено 85 различных жертв, принадлежащих к семи сообществам.



Кроме того, вредоносные серверы содержат видеофайлы, которые захватывают деятельность на видео. Хотя видео хранятся в сжатом формате, который обеспечивает низкое качество изображения, выбранный формат минимизирует загрузку полосы пропускания и имеет достаточное качество, чтобы злоумышленники могли понять действия жертв. В соглашениях об именах видеофайлов используется имя приложения в передний план (например, Outlook, Cmd и т. д.) и только записанная активность

пользователя. Это помогло злоумышленникам необходимо как перейти к интересующим файлам, так и удалить лишние файлы. Используя данные, полученные с помощью видео и других методов мониторинга, злоумышленники составили оперативную картину рабочего процесса жертвы, инструментов и практики. Эта картинка помогает злоумышленникам развернуть свои вредоносные операции.

Например: злоумышленники создали поддельные транзакции во внутренней базе данных жертвы после процесс проверки, что позволяет избежать обнаружения мошеннической деятельности; Злоумышленники использовали внутренние командные утилиты жертвы для вставки мошеннических операции в очереди транзакций.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Index	Random Keys								KVC	KVC of Key	ATM
2		FE								CC		
3	102	89								B3		
4		D5								16		
5	103	62								F3		
6		B6								86		
7	104	BA								DE		
8		AE								27		
9	105	DC								BD		
10		5B								E7		
11	106	54								7A		
12		92								B8		
13	107	B6								3B		
14		04								E9		
15	108	9B								02		
16		07								D6		
17	109	E5								50		
18		AB								6C		
19	110	DC								EA		
20		8C								7E		
21	111	51								41		
22		08								E5		
23	112	4C								E5		
24		20								34		
25	113	F8								BF		
26		CD								8F		
27	114	68								FE		
28		B9								B6		
29	115	75								EA		
30		B5								92		
31	116	7F								36		
32		D0								EE		
33	117	4F								56		
34		BA								EE		
35	118	B3								9C		
36		4C								4F		
37	119	1C								FB		
38		25								7D		

Список PIN-кодов KVC, используемых в банкоматах

Конфиденциальные банковские документы были обнаружены на серверах, которые контролировали Carbanak . Они включали секретные электронные

письма, руководства, криптоключи, пароли. и так далее. Например, файл на рисунке выше имеет KVC (коды проверки ключей). ключи, которые используются банкоматами для проверки целостности ПИН-кодов своих пользователей. В других случаях, связанных с банкоматами, преступники могли контролировать компьютеры, которые имел доступ к внутренней сети банкоматов. Если в банке включен удаленный доступ к банкоматам преступники начали использовать этот доступ для удаленного снятия наличных. Злоумышленники не использовали вредоносное ПО для работы банкомата; вместо этого они использовали стандартные утилиты для контроля и тестирования банкоматов.

Вывод: исходный код CARBANAK иллюстрирует, как авторы этих вредоносных программ решили некоторые практические проблемы обфускации. И код задач, и система разрешения Windows API представляют собой значительные вложения, чтобы избавить аналитиков вредоносных программ от следов бэкдора.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с основными угрозами и атаками на АТМ, а также с методами их защиты.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

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
5. Advance Persistent Threat Detection Using Long Short Term Memory (LSTM)Neural Networks [Электронный источник] – URL: https://www.researchgate.net/
6. Scenario-based cyber attack defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network [Электронный источник] – URL: https://www.researchgate.net/
7. Информационная безопасность банкоматов [Электронный источник] – URL: https://elibrary.ru/