УДК 004.491.42

ИССЛЕДОВАНИЕ И АНАЛИЗ КОДА НАИБОЛЕЕ ПОПУЛЯРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ ТИПА «БЛОКИРАТОР-ШИФРОВАЛЬЩИК ФАЙЛОВ»

Е.Б. Дроботун, к.т.н., докторант, drobotun@xakep.ru
(Военная академия воздушно-космической обороны им. Маршала Советского Союза Г.К. Жукова, ул. Жигарева, 50, г. Тверь, 170022, Россия)

Аннотация. Компании, занимающиеся разработкой антивирусного программного обеспечения, отметили с середины 2013 года всплеск заражений компьютеров вредоносными программами, шифрующими пользовательскую информацию, – наиболее опасной разновидностью вредоносных программ класса Ransomware (программ-вымогателей). Программы такого рода не просто блокируют доступ пользователей к компьютеру, а шифруют файлы, представляющие для них наибольшую ценность (документы, фотографии и т.п.), и требуют выкуп за восстановление. В статье приведены результаты анализа кода нескольких представителей этого класса вредоносных программ, показаны основные тенденции развития такого рода программ и предложены возможные пути устранения последствий их деятельности.

Ключевые слова: *вредоносная программа, шифрование, кибервымогательство, компьютерные вирусы, борьба с компьютерными вирусами.*

Первые сообщения о появлении нового семейства вредоносных программ, шифрующих файлы пользователей и требующих выкупа за их расшифровку, датируются 2006–2007 годами. Однако на тот момент в силу различных причин (неотработанность каналов распространения создателями таких программ, несовершенство реализации алгоритмов шифрования и способов оплаты выкупа и т.п.) количество заражений этими вредоносными программами было относительно небольшим.

Массовый характер заражения такого рода вредоносными программами стали приобретать с 3-го квартала 2013 года, а за 2014 год, по данным «Лаборатории Касперского», было зарегистрировано свыше 7 000 000 атак на пользователей с помощью программ этого типа (рис. 1) [1].

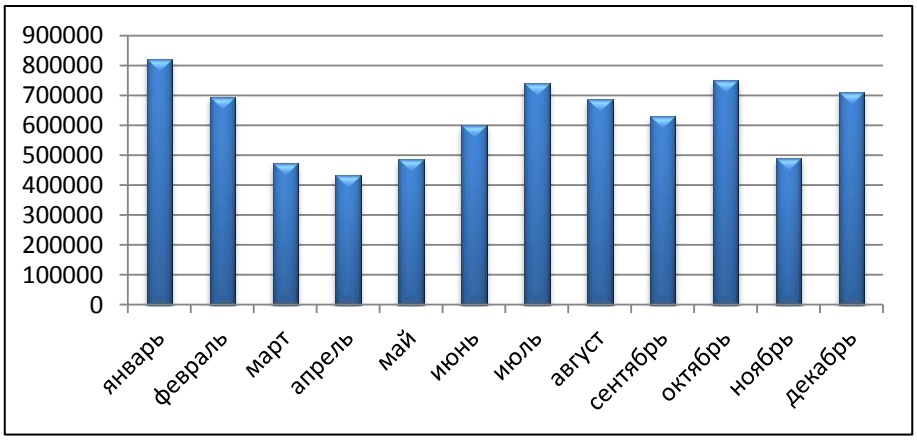

Рис. 1. Количество атак с использованием вредоносных программ-шифровальщиков за 2014 год (по данным «Лаборатории Касперского»)

Всеми антивирусными компаниями также отмечен значительный рост числа модификаций вредоносных программ этого типа в период с 2013 по 2015 годы. Так, например, по данным компании «Лаборатория Касперского», за отмеченный период число модификаций таких программ возросло более чем в десять раз (рис. 2) [2].

При этом, если первоначально все вредоносные программы такого рода разрабатывались исключительно для функционирования под операционными системами семейства Windows, то в дальнейшем, начиная с середины 2014 года, появились модификации этих программ для смартфонов и планшетных компьютеров под управлением операционной системы Android, а в конце 2015 года было зафиксировано появление нескольких образцов вредоносных программ-шифровальщиков для компьютеров под управлением операционными системами семейства Linux [2].

Тем не менее, в силу меньшей распространенности и некоторых особенностей функционирования других операционных систем подавляющее большинство случаев заражения вредоносными программа-

ми-шифровальщиками (порядка 98 %) приходится на компьютеры под управлением операционных систем семейства Windows.

Первое время основным каналом распространения таких вредоносных программ были спам-рассылки с вредоносными вложениями, маскирующимися под какие-либо документы (финансовые отчеты, банковские выписки по счетам, отчеты от служб доставки и т.п.) [3, 4].

В начале 2014 года к спам-рассылкам добавился канал распространения с помощью заражения популярных и часто посещаемых веб-страниц так называемыми наборами эксплойтов (эксплойт-паками) [3]. Их работа основана на использовании уязвимостей в программном обеспечении, установленном на компьютерах потенциальных жертв. Наиболее часто для распространения этих вредоносных программ используются наборы эксплойтов под названием Angler EK, Sweet Orange EK и Nuclear EK [5, 6].

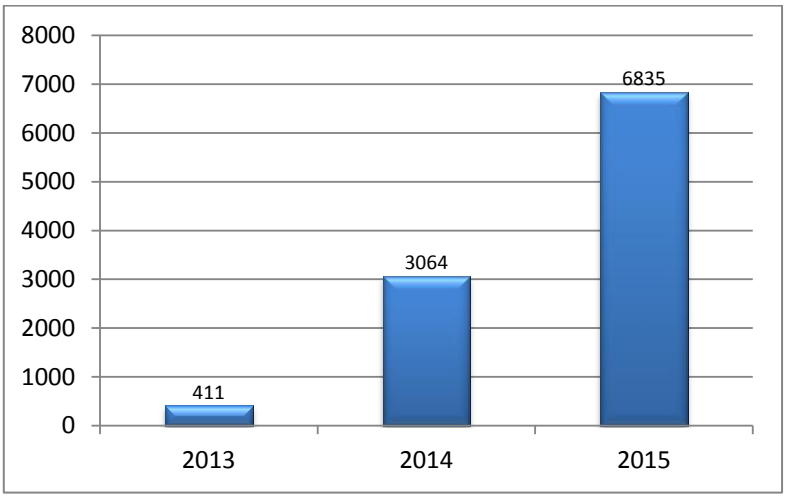

Рис. 2. Рост числа модификаций вредоносных программ-шифровальщиков в период с 2013 по 2015 гг. (по данным «Лаборатории Касперского»)

Общая схема работы вредоносных программ-шифровальщиков представлена на рисунке 3. После проникновения на компьютер потенциальной жертвы вредоносная программа записывает себя на жесткий диск компьютера, далее для обеспечения своего запуска при старте системы создает ключ автозагрузки в реестре, после чего производятся поиск нужных файлов и их шифрование. Далее устанавливается связь с командным (C&C) сервером. После всего этого программа оповещает жертву о том, что определенные файлы на компьютере зашифрованы, и требует произвести оплату за их расшифровку. Для оплаты, как правило, предлагается воспользоваться каким-либо сервисом интернет-платежей или произвести оплату с помощью какой-либо криптовалюты (в большинстве случаев – биткойнами). После подтверждения факта оплаты производится расшифровка файлов.

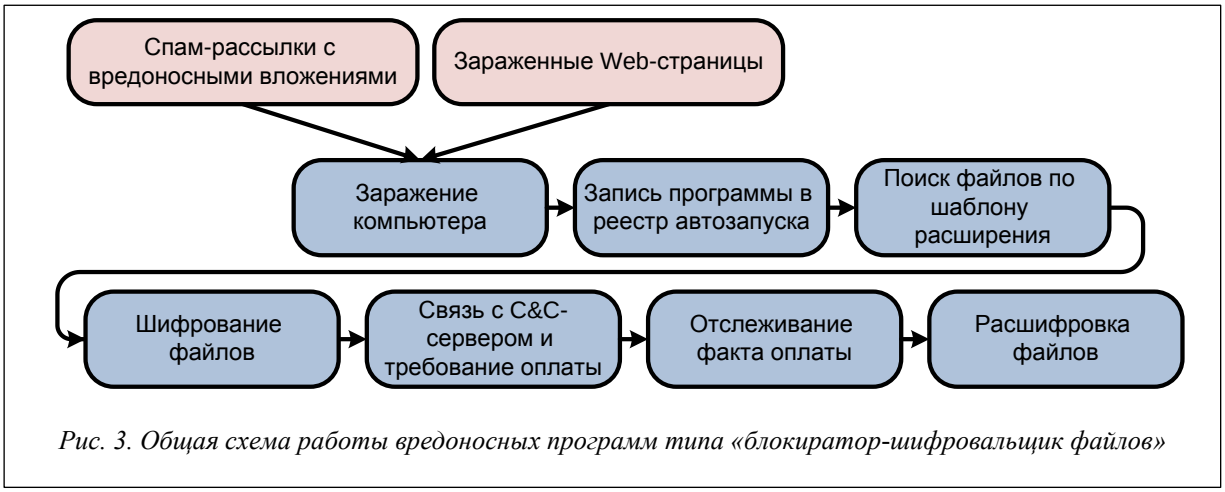

Рис. 3. Общая схема работы вредоносных программ типа «блокиратор-шифровальщик файлов»

Наибольшую активность с середины 2013 года и по настоящее время проявляли семь видов вредоносных программ-шифровальщиков файлов (см. таблицу) [3, 6, 7].

Вредоносные программы типа «блокиратор-шифровальщик файлов», проявившие наибольшую активность с середины 2013 года по настоящее время

№ п/п	Название вредоносной программы	Название вредоносной программы по классификации «Лаборатории Касперского»	Контрольная сумма исследуемого образца вредоносной программы (MD5-хэш)
1	DyrCrypt (Dirty)	Trojan-Ransom.Win32.Dircrypt	7a3c8d7f8b2b5bd26995dd33f4c1ee3ch
2	CryptoLocker	Trojan-Ransom.Win32.Blocker	2a1609ef72f07abc97092cb456998e43h
3	CryptoWall	Trojan-Ransom.Win32.Blocker	73a9ab2ea9ec4eaf45bce88afc7ee87eh
4	Critroni (CTB-Locker)	Trojan-Ransom.Win32.Onion	e89f09fdded777ceba6412d55ce9d3bch
5	TorrentLocker	Trojan-Ransom.Win32.Rack	93cbe4ed3d46abe732a124a41e7147a2h
6	TorLocker	Trojan-Ransom.Win32.Scraper	afeb4f5d627443eedb127708262253dfh
7	TeslaCrypt (AlphaCrypt)	Trojan-Ransom.Win32.Bitman	388fc7a1de13ec2345c18893be62d965h

Общая хронология появления этих семи вредоносных программ показана на рисунке 4 [1, 3, 6].

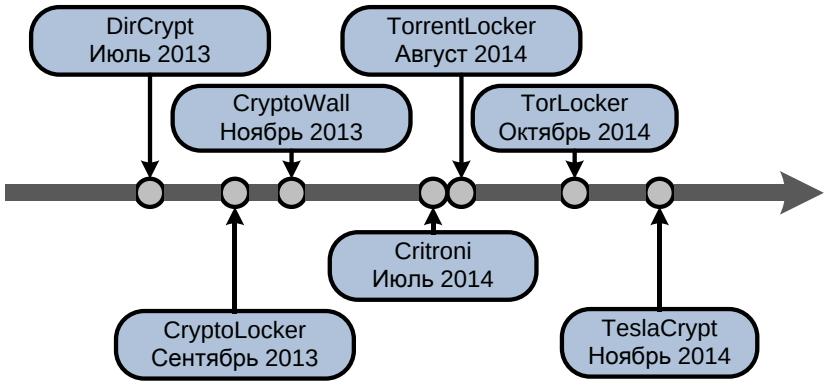

Рис. 4. Хронология появления вредоносных программ-шифровальщиков файлов

Их исследования проводились путем анализа кода вредоносных программ с использованием отладчиков и дизассемблера (OllyDbg, WinDbg, IdaPro) и путем запуска исследуемых вредоносных программ в виртуальной среде, созданной с помощью системы виртуализации Oracle Virtual Box с контролем вызываемых API-функций Windows с использованием программы API-Monitor по следующей схеме:

- исследование и анализ путей распространения программы и процесса заражения компьютера;
- исследование и анализ используемых алгоритмов шифрования файлов;
- исследование и анализ способов связи и структуры обмена с командным сервером;
- исследование и анализ приемов, затрудняющих обнаружение и анализ программы.

DirCrypt (Trojan-Ransom.Win32.Dircrypt). Данная вредоносная программа появилась в середине 2013 года. Основной способ ее распространения – спам-рассылки с вредоносным вложением, замаскированным под документ в формате RTF [8].

Отбор файлов для шифрования производится по их расширениям. Программа шифрует файлы следующих типов: *.jpg, *.jpeg, *.png, *.avi, *.mpeg, *.mpg, *.wmv, *.doc, *.rtf, *.zip, *.7z, *.pdf, *.docx, *.docm, *.xls, *.xlsx, *.xlsm. Для шифрования файлов на зараженном компьютере применяются два алгоритма – RC-4 и RSA-1024. При этом алгоритмом RSA-1024 с помощью публичного ключа, содержащегося непосредственно в теле вредоносной программы, шифруются первые 1024 байта файла, а с помощью алгоритма RC-4 – остальная часть файла, при этом ключ шифрования генерируется по псевдослучайному закону (один для всех шифруемых файлов) и записывается в конец зашифрованного файла [7, 9]. После зашифровывания всех файлов программа меняет обои рабочего стола компьютера на картинку с требованием выкупа (рис. 5).

Связь с командным сервером осуществляется по протоколу HTTP, при этом доменные имена командных центров программа генерирует самостоятельно с помощью специального алгоритма на основе двух четырехбайтовых начальных чисел, находящегося в секции ресурсов программы (рис. 6). Всего может быть сгенерировано до 30 доменных имен, которые представляют собой набор случайных символов [7]. После генерации очередного доменного имени производится попытка установить связь с C&C-сервером. В случае успеха такой попытки и после зашифровывания всех файлов на компьютере жертвы публичный

Рис. 5. Требование оплаты выкупа за расшифровку файлов вредоносной программой DirCrypt

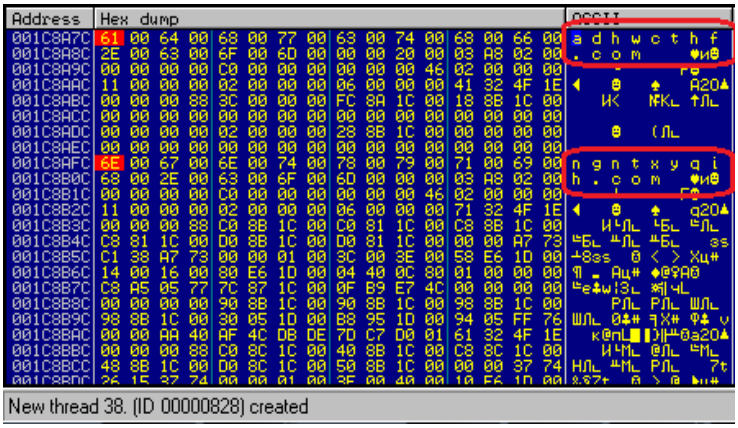

Рис. 6. Работа алгоритма генерации доменных имен командного сервера вредоносной программы DirCrypt (выделены два сгенерированных доменных имени: adhwcthf.com и ngntxqih.com)

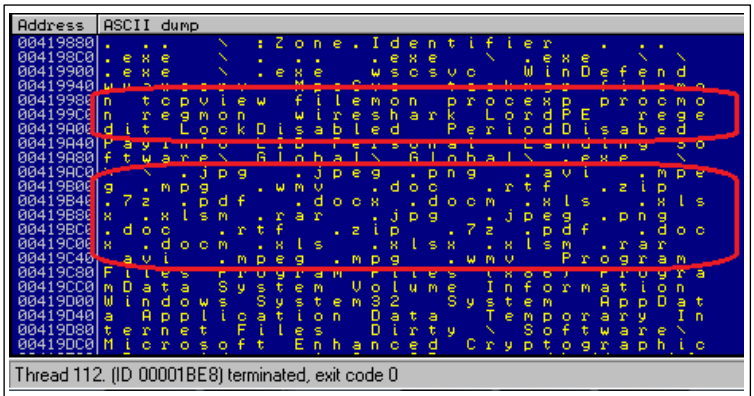

Рис. 7. Расшифрованные текстовые строки в теле вредоносной программы DirCrypt (выделены названия программ, запуску которых препятствует DirCrypt, и маски, по которым отбираются файлы для шифрования)

ключ RSA-алгоритма, содержащийся в теле программы, пересылается на командный сервер для получения приватного RSA-ключа после подтверждения факта оплаты.

Для затруднения обнаружения и анализа работы DirCrypt постоянно осуществляет поиск запущенных процессов некоторых системных утилит (рис. 7). Для обнаружения этих процессов используются API-функции CreateToolhelp32Snapshot, Process32First и Process32Next. После обнаружения таких процессов производятся остановка и завершение их с помощью API-функции TerminateProcess. Помимо этого, для затруднения анализа программы все текстовые строки и данные, необходимые для работы, хранятся в зашифрованном виде, а их расшифровка производится по мере обращения к этим данным. На рисунке 7 показаны некоторые текстовые строки в теле вредоносной программы уже в открытом виде.

Вредоносная программа DirCrypt (Dirty) – первая программа, шифрующая файлы пользователя и требующая выкуп за возможность расшифровать файлы, заражение которой приобрело достаточно массовый характер.

Однако использование алгоритма шифрования RC-4 и сохранение ключа шифрования в конце зашифрованного файла позволяют достаточно просто восстанавливать зашифрованные файлы (даже несмотря на RSA-шифрование первых 1024 байт файла). К примеру, все файлы документов Microsoft Office имеют в начале одинаковый для всех типов файлов заголовок, длина которого больше 1024 байт, что позволяет восстановить такие файлы без потерь [9].

CryptoLocker (Trojan-Ransom.Win32.Blocker). Первые факты заражения этой вредоносной программой были зафиксированы в начале сентября 2013 года (первый образец вредоносной программы этого семейства был загружен на антивирусный сервис virustotal.com 8 сентября 2013 года). За первые три месяца с момента своего появления программа заразила порядка 250 тысяч компьютеров (преимущественно в США) [10].

Распространяется эта вредоносная программа посредством спам-рассылок, в большинстве случаев от имени служб доставки Fedex или UPS

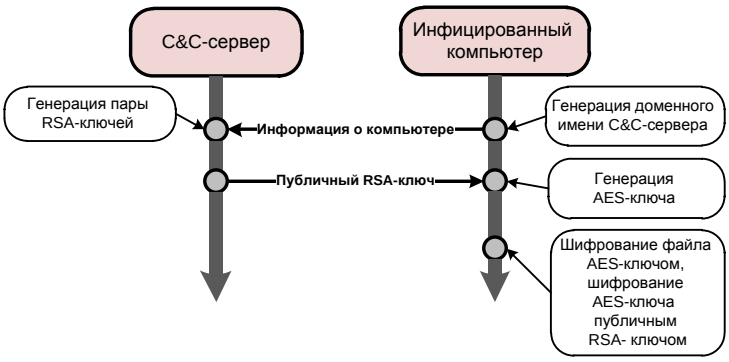

Рис. 8. Общая схема процесса шифрования файлов вредоносной программой CryptoLocker

под видом отчета о доставке товара [11].

Файлы для шифрования отбираются исходя из их расширения. Всего этой вредоносной программой могут быть зашифрованы 72 типа файлов (документы MS Office и Open Office, файлы изображений, файлы систем проектирования и работы с базами данных). Общая схема процесса шифрования файлов, реализованного в CryptoLocker, показана на рисунке 8. Для шифрования используется симметричный алгоритм AES-256, для реализации которого использованы возможности стандартной библиотеки CryptoAPI [10, 11].

После шифрования файлов ключ AES-алгоритма, с помощью которого они были зашифрованы, шифруется с помощью алгоритма RSA-2048 с использованием публичного ключа, полученного от командного сервера. Далее зашифрованный AES-ключ пишется в начало зашифрованного файла. Помимо зашифрованного AES-ключа, в начало файла в виде SHA-хэша длиной 20 байт записывается контрольная сумма публичного RSA-ключа (это дает возможность в случае оплаты выкупа найти на командном сервере нужный приватный RSA-ключ). В итоге длина зашифрованного файла увеличивается на 276 байт по сравнению с исходным незашифрованным файлом (рис. 9).

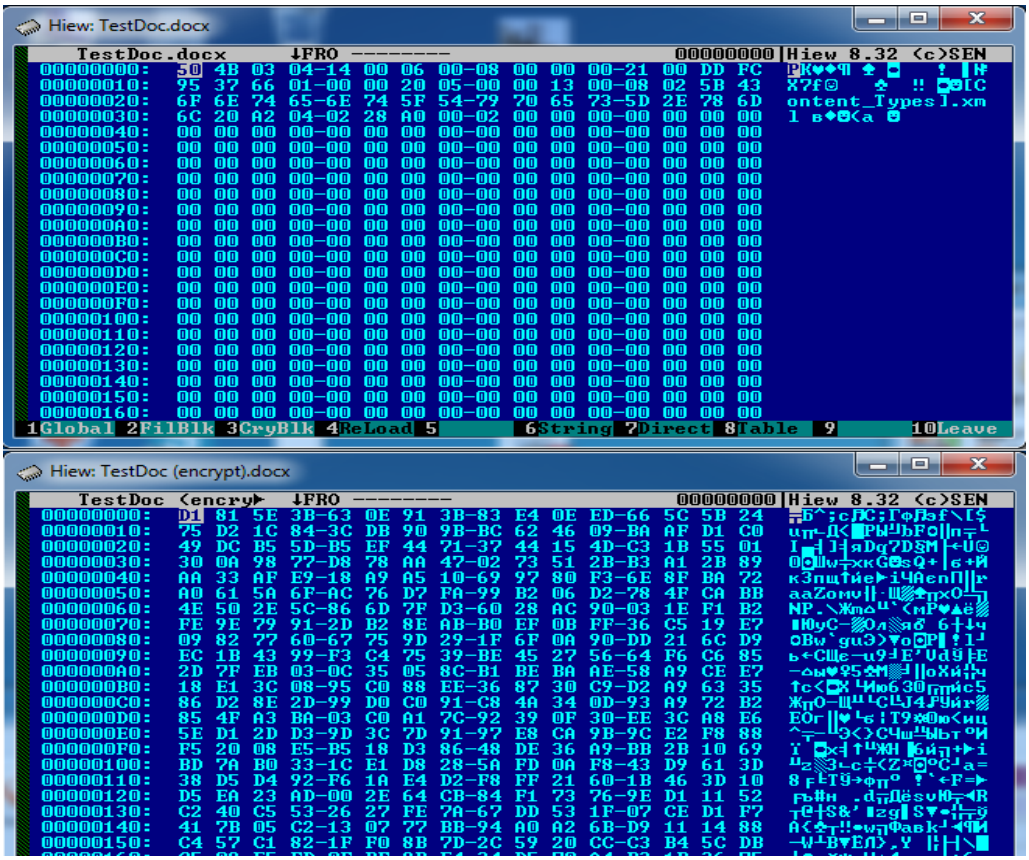

Рис. 9. Зашифрованный вредоносной программой CryptoLocker файл (внизу) и исходный (незашифрованный) файл TestDoc.docx (вверху)

Генерация доменного имени командного сервера в данной вредоносной программе реализуется посредством алгоритма, основанного на API-функции GetSystemTime (рис. 10).

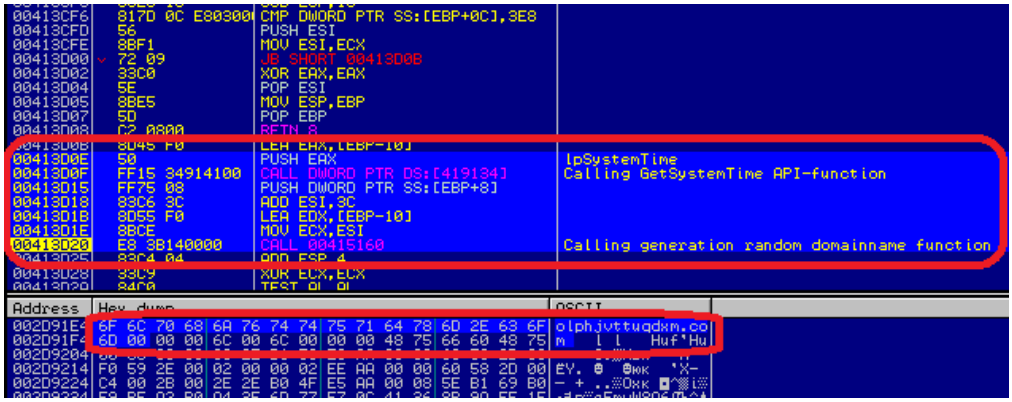

Рис. 10. Работа алгоритма генерации доменного имени командного центра вредоносной программы CryptoLocker (в нижней части выделено сгенерированное доменное имя olphjvttuqdxm.com)

Генерация доменных имен и попытки подключения к ним продолжаются до момента установления успешного соединения (то есть было сгенерировано имя действующего на данный момент C&C-сервера), после чего на командный сервер отсылается информация о зараженном компьютере, собранная ранее, а на сервере генерируется пара RSA-ключей (публичный и приватный). Публичный RSA-ключ отсылается на зараженный компьютер, где он сохраняется в реестре, в специально созданном на первом этапе заражения разделе, и далее используется при зашифровке файлов [11].

Рис. 11. Окно с требованием оплаты выкупа за расшифровку файлов вредоносной программой CryptoLocker

После зашифровывания всех файлов на компьютере жертвы выводится окно с предупреждением о том, что файлы зашифрованы, и с требованием оплатить выкуп за возможность расшифровать эти файлы (рис. 11). Для оплаты выкупа предлагается воспользоваться системой платежей MoneyPak либо перечислить средства через биткойн-кошелек.

Программа не использует никакие средства защиты от обнаружения и анализа, за исключением запуска дублирующего процесса, который контролирует работу основного и в случае его остановки осуществляет повторный запуск.

CryptoLocker – первая вредоносная программа из семейства блокираторов-шифровальщиков файлов, появление и некоторые факты заражения которой получили очень широкую огласку в различных средствах массовой информации [6, 12].

Данная вредоносная программа, в отличие от ранее появившихся образцов программ такого рода, использует очень стойкую криптографию на базе симметричного алгоритма AES-256 для шифрования файлов и на базе ассиметричного алгоритма RSA-2048 для шифрования AES-ключа. Взлом такой схемы шифрования возможен только путем перебора всех возможных вариантов приватного RSA-ключа, а использование достаточно длинных ключей не позволяет подобрать нужный ключ за приемлемое время.

Помимо этого, в данной вредоносной программе в качестве одного из вариантов оплаты выкупа впервые была использована криптовалюта биткойн, что практически исключает возможность отследить получателей платежей и привлечь их к ответственности.

CryptoWall (Trojan-Ransom.Win32.Blocker). Массовое распространение этой вредоносной программы зафиксировано в начале 2014 года, однако первые образцы были обнаружены еще в ноябре 2013 года. В этом семействе вредоносных программ известны две версии – CryptoWall 2.0 и CryptoWall 3.0. В настоящее время версия 3.0 активно применяется злоумышленниками, и количество заражений этой

программой остается достаточно высоким. Распространение данной вредоносной программы осуществляется с зараженных веб-страниц с применением наборов эксплойтов Angler EK и Nuclear EK [7].

Список шифруемых файлов у этой вредоносной программы довольно широк, и, помимо документов, фотографий, видео, архивов, данная программа шифрует файлы проектов различных средств разработки программного обеспечения.

Для шифрования файлов используется RSA-алгоритм с длиной ключа 2048 бит, при этом, в отличие от большинства других вредоносных программ этого типа, RSA-алгоритмом шифруется непосредственно содержимое файла, а не ключ AES-алгоритма, которым и были зашифрованы файлы [13].

Общая схема заражения компьютера представлена на рисунке 12. После срабатывания эксплойта на зараженной веб-странице производится загрузка самой вредоносной программы, при этом следует отметить, что для затруднения обнаружения и анализа файлов этой вредоносной программы ее код подвергнут многоуровневой упаковке и шифрованию.

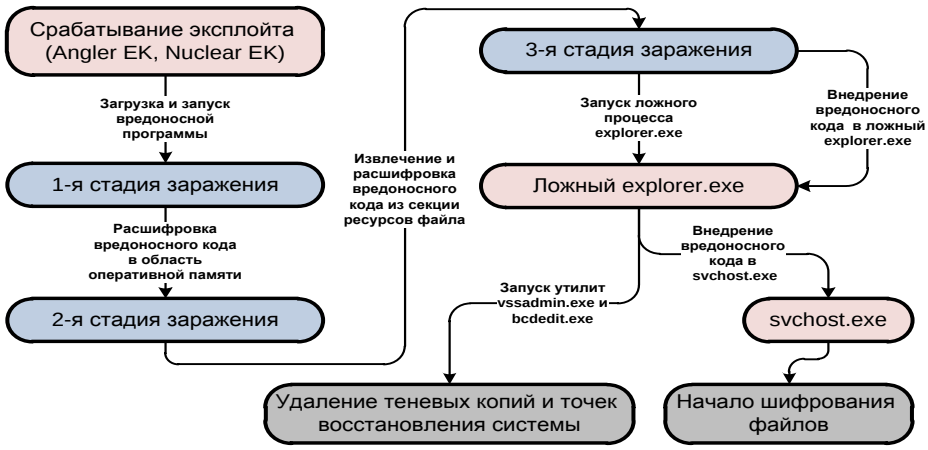

Рис. 12. Последовательность распаковки и запуска процессов вредоносной программы CryptoWall

На первой стадии заражения компьютера производится запуск загруженного с зараженной веб-страницы вредоносного кода. Далее, на второй стадии, производятся извлечение и расшифровка в оперативную память из загруженного кода основных компонентов вредоносной программы в виде образа исполняемого файла, в секции ресурсов которого размещаются непосредственно сами компоненты вредоносной программы. На третьей стадии заражения инициируется запуск ложного процесса explorer.exe, в который производится внедрение вредоносного кода, извлеченного из секции ресурсов. Далее из этого процесса explorer.exe запускаются стандартные утилиты vssadmin.exe и bcdedit.exe для удаления всех точек восстановления системы и стирания всех теневых копий файлов пользователя для исключения возможности восстановления зашифрованной информации из теневых резервных копий и точек восстановления системы [7, 14].

Связь с командными серверами может осуществляться либо посредством анонимной сети tor (для этого из сети Интернет загружается и устанавливается клиент tor.exe), либо через анонимную сеть I2P. Все имена командных серверов прописаны непосредственно в теле вредоносной программы, а связь осуществляется с шифрованием передаваемых данных по алгоритму RC4. От командного сервера передается публичный RSA-ключ (на третьем этапе заражения, после внедрения вредоносного кода в процесс svchost.exe), и далее с его помощью начинается шифрование файлов.

В версии CryptoWall 2.0 на втором этапе производится проверка на наличие виртуального окружения путем поиска процессов VBoxService.exe, vmtoolsd.exe (наличие которых характерно при использовании виртуальной машины Virtual Box) или загруженной библиотеки sbieDLL.dll (эта библиотека присутствует в системе с запущенной средой виртуализации SandBox) (рис. 13) [14].

Вредоносная программа CryptoWall, как и CryptoLocker, использует стойкий к взлому криптографический алгоритм, исключающий всякую возможность восстановления файлов без знания приватного RSA-ключа. Для исключения возможности отслеживания командных серверов в сети Интернет создатели этой вредоносной программы размещают командные серверы в анонимной доменной зоне .onion сети tor (или используют анонимную сеть I2P).

На сегодняшний день антивирусные компании продолжают фиксировать большое количество заражений этой вредоносной программой.

Critroni (CTB-Locker) (Trojan-Ransom.Win32.Onion). Программа появилась в начале февраля 2014 года [15]. В отличие от предшествующих вредоносных программ-шифровальщиков здесь использована

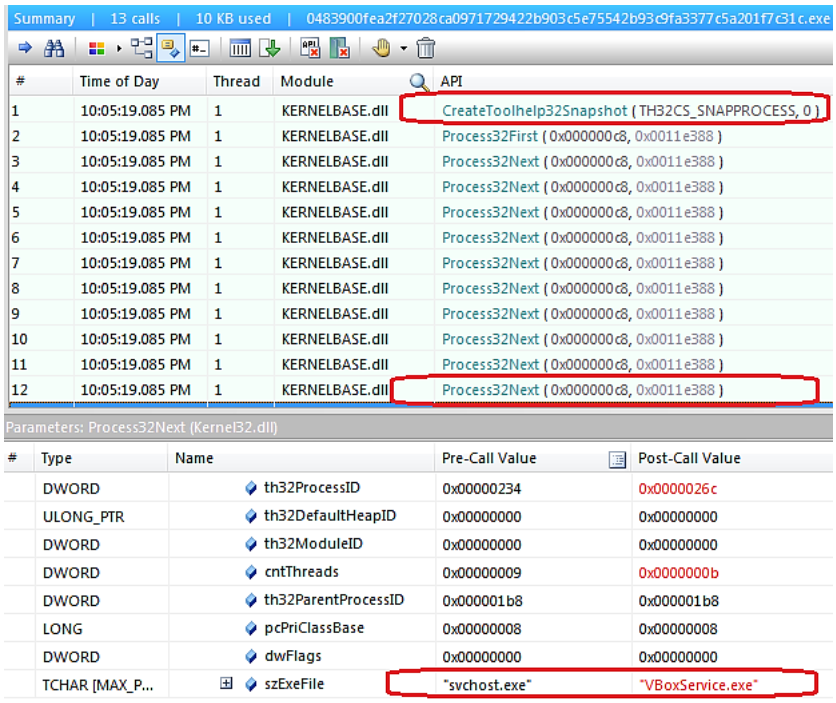

Рис. 13. Поиск процесса VBoxService.exe для обнаружения виртуальной машины Virtual Box во вредоносной программе CryptoWall версии 2.0

новая схема шифрования файлов с использованием алгоритма Диффи-Хеллмана на эллиптических кривых (ECDH – Ellipticcurve Diffie-Hellman).

Шифрованию подвергаются файлы следующих типов: *.xlsx, *.xlsm, *.xlsb, *.xls, *.xlk, *.txt, *.sql, *.safe, *.rtf, *.pwm, *.pem, *.mdf, *.mdb, *.kwm, *.groups, *.docx, *.docm, *.doc, *.der, *.dbf, *.db, *.crt, *.cer. Само шифрование производится в несколько этапов (рис. 14). Особенность реализации процесса шифрования файлов в этой вредоносной программе (помимо использования криптографического алгоритма на эллиптических кривых) заключается в том, что перед шифрованием файла дополнительно производится его поблочное сжатие, после чего уже сжатые блоки шифруются и записываются на место оригинального файла. Сжатие производится с помощью функции deflate из свободно распространяемой библиотеки Zlib. После шифрования всех файлов на экран компьютера выводится окно с требованием оплаты выкупа и инструкцией по дальнейшим действиям (рис. 15).

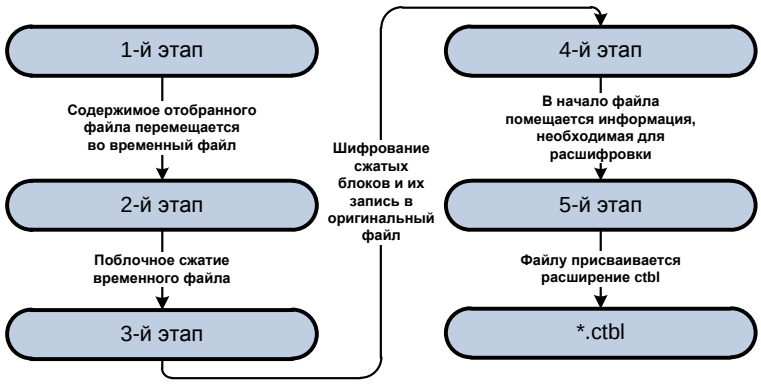

Рис. 14. Общая схема процесса шифрования файлов вредоносной программой Critroni (CTB-Locker)

Перед началом шифрования файлов генерируется пара ключей для RSA-алгоритма (публичный – master-public и приватный – master-private), при этом master-private на зараженном компьютере не сохраняется, а отправляется на C&C-сервер (перед отправкой этот ключ шифруется с помощью алгоритма

Рис. 15. Окно с требованием оплаты выкупа за расшифровку файлов вредоносной программой Critroni

ECDH). Ключи генерируются на основе 34-байтного случайного числа, состоящего из шести чисел, которые являются результатом выполнения некоторых API-функций Windows [16].

Все командные серверы этой вредоносной программы находятся в доменной зоне .onion анонимной сети tor, при этом доменное имя C&C-сервера прописано непосредственно в теле программы (рис. 16).

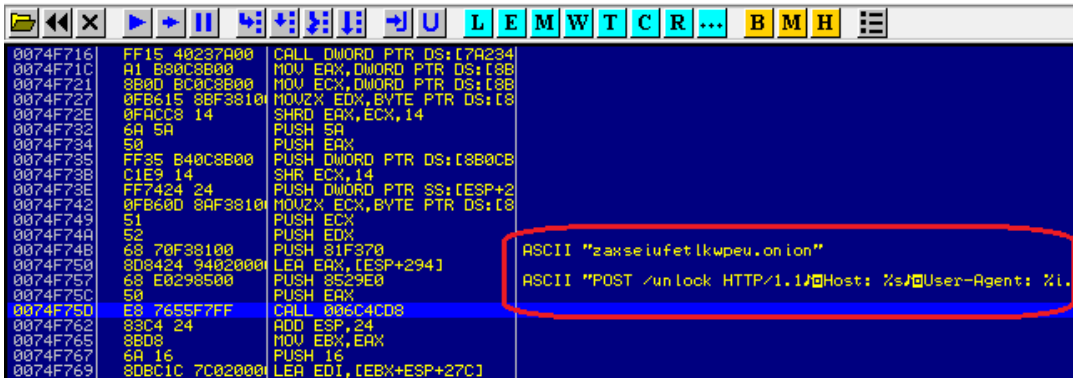

Рис. 16. Фрагмент кода tor-клиента в теле вредоносной программы Critroni (CTB-Locker) (выделены имя C&C-сервера и сформированный запрос на C&C-сервер)

Связь с командным центром осуществляется с помощью встроенного в программу tor-клиента, код которого практически без изменения взят из открытых источников [15]. Весь обмен с командным сервером происходит в закрытом виде (все команды и сообщения шифруются с помощью ECDH-алгоритма).

CTB-Locker является весьма развитой и качественно реализованной (с точки зрения написания кода и реализации функционала) вредоносной программой. Использование нетипичной и не применяемой ранее схемы шифрования файлов позволило добиться весьма стойкого шифрования, при этом скорость работы реализованных алгоритмов шифрования оказалась гораздо выше, чем у появившихся ранее вредоносных программ такого рода. Использование tor-клиента, реализованного непосредственно в теле программы, позволило минимизировать обмен с командным сервером, а использование сети tor и способа оплаты с помощью биткойнов – достичь практически полной анонимности злоумышленников, распространяющих эту вредоносную программу.

TorrentLocker (Trojan-Ransom.Win32.Rack). Первые факты заражения этой вредоносной программой были зафиксированы в феврале 2014 года. Программа распространяется исключительно в виде вложений в письмах спам-рассылок от имени различных финансовых организаций.

Данная программа шифрует большое количество различных файлов (порядка 250 типов, в том числе и файлы бухгалтерских программ 1С) [17], что позволяет парализовать работу многих организаций, подвергшихся заражению этой вредоносной программой.

Для шифрования файлов используется алгоритм AES-256. Ключ шифрования генерируется один раз на основе значений, получаемых в результате работы нескольких API-функций Windows [18]. После шифрования файлов AES-ключ шифруется публичным ключом RSA, который находится в файле вредоносной программы и записывается в конец зашифрованного файла вместе с контрольной суммой AES-ключа и значением длины зашифрованного AES-ключа. Если шифруемый файл больше 2 МБ, для снижения нагрузки на процессор и уменьшения времени шифруются только первые 2 МБ файла. Для реализации алгоритмов шифрования применяется свободно распространяемая библиотека LibTomCrypt [7].

Помимо шифрования файлов, эта вредоносная программа осуществляет кражу данных из адресных книг различных почтовых программ на зараженном компьютере. Учитывая способ распространения этой программы, можно сделать вывод, что благодаря этому создателям программы удается существенно увеличить число заражений компьютеров этой программой и расширить область ее распространения [19].

Для связи с командным сервером программа использует доменное имя, прописанное в теле программы (хотя более поздние версии могут иметь в своем составе алгоритм генерации доменных имен дополнительно к доменному имени C&C-сервера, прописанному в теле вредоносной программы). Вся передаваемая по сети информация шифруется с помощью SSL-протокола. На командный сервер передается информация, позволяющая идентифицировать пользователя (она вырабатывается из имени компьютера, даты установки системы и версии ОС). Этот идентификатор позволяет впоследствии установить факт оплаты (оплата возможна с помощью криптовалюты биткойн) и предоставить возможность расшифровки файлов.

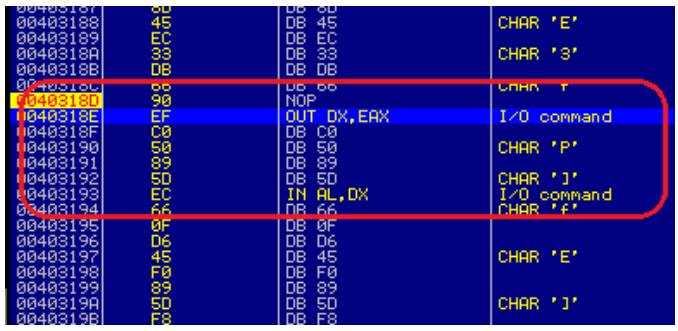

Рис. 17. Обнаружение факта запуска вредоносной программы TorrentLocker в виртуальном окружении (с использованием привилегированных команд процессора)

В данной вредоносной программе применены несколько приемов, направленных на затруднение ее анализа. Первый позволяет обнаруживать факт запуска программы в виртуальном окружении (рис. 17), второй делает невозможным запуск программы под отладчиком OllyDbg или WinDbg (рис. 18). В первом случае используются привилегированные команды процессора, во втором – особенности выполнения API-функции OutputDebugString.

Для скрытия факта своего присутствия в зараженной системе данная программа внедряет вредоносный код в процесс explorer.exe в виде удаленного потока и осуществляет свои действия под прикрытием этого процесса.

Самое главное отличие этой вредоносной программы от других программ такого рода – похищение информации из адресных книг почтовых клиентов, установленных на зараженные компьютеры. Похищенная информация использовалась с целью расширения области заражения данной вредоносной программой и увеличения количества жертв заражений этой программой.

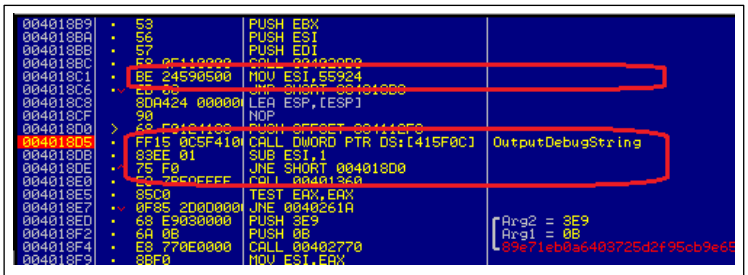

Рис. 18. Обнаружение факта запуска вредоносной программы TorrentLocker под отладчиком (с использованием особенностей API-функции OutputDebugString)

TorLocker (Trojan-Ransom.Win32.Scraper). Первый факт заражения этой программой был зафиксирован в октябре 2014 года. Данная вредоносная программа представлена двумя версиями: версией 1.0 на английском языке и 2.0 на английском и японском языках (рис. 19). Основное различие между версиями заключается в методах затруднения анализа кода и используемом источнике дополнительных модулей: в версии 2.0 эти модули загружаются из сети Интернет, в версии 1.0 они извлекаются из секции данных.

Рис. 19. Окно с требованием оплаты выкупа вредоносной программы TorLocker версии 2.0

Программа шифрует большое количество типов файлов (офисные документы, аудио- и видеозаписи, изображения, файлы архивов, файлы проектов различных сред программирования, файлы виртуальных машин и т.п.).

Файлы шифруются алгоритмом AES-256, при этом для каждого из них генерируется свой ключ шифрования. Если размер файла больше 512 МБ, шифруются только первые 512 МБ файла. AES-ключ шифруется с помощью алгоритма RSA-2048 (ключ для него на основании имени компьютера и серийного номера логического диска выбирается из 128 публичных RSA-ключей, прописанных в теле программы). В конец каждого файла дописывается служебная информация размером 512 байт. При шифровании зашифрованные данные записываются в файл поверх незашифрованных, а создание нового файла с удалением старого не происходит. Названия и расширения зашифрованных файлов не изменяются [20].

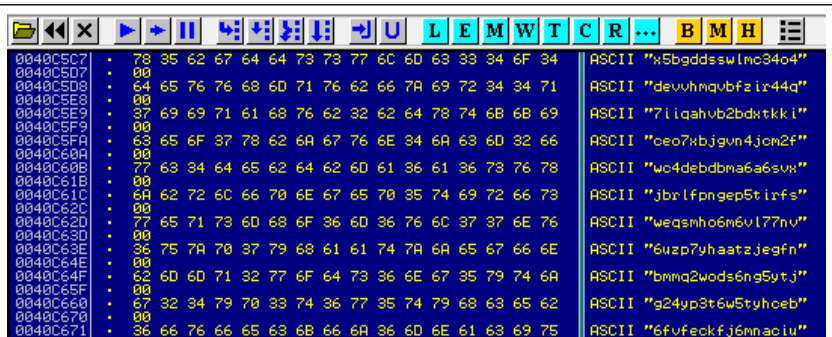

Рис. 20. Имена командных серверов в теле вредоносной программы TorLocker

Связь с командным сервером устанавливается уже после того, как все файлы будут зашифрованы. Этим достигаются скрытность работы вредоносной программы и невозможность выявления его работы по нетипичной сетевой активности. Все адреса командных серверов прописаны в теле программы (рис. 20), связь с ними осуществляется посредством tor-клиента tor.exe и с использованием прокси-сервера polipo.exe. Эти два файла либо извлекаются из секции данных (в версии 1.0), либо загружаются из сети Интернет (в версии 2.0) (рис. 21) [7].

В большинстве случаев код вредоносной программы упакован с помощью упаковщика UPX. Также для затруднения анализа в коде программы имеется большое количество ничего не значащих команд (так называемые «висячие байты»).

Программа запускает отдельный поток, в котором отслеживает запуск процессов различных утилит анализа системы (taskmgr.exe, regedit.exe, procexp.exe, procexp64.exe) и при обнаружении завершает эти процессы (по аналогии с вредоносной программой DirCrypt).

В данной вредоносной программе используется связка стойких к взлому алгоритмов AES-256 и RSA-2048 (по аналогии, например, с вредоносной программой CryptoLocker), однако, несмотря на это, в первоначальных образцах этой программы криптографические алгоритмы были реализованы с ошибкой, что во многих случаях позволяло расшифровывать файлы без обращения к создателям этой программы [20].

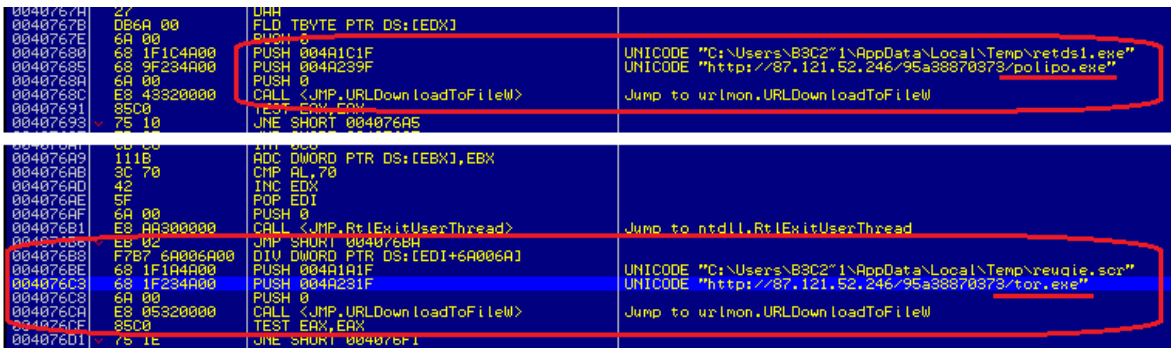

Рис. 21. Загрузка tor-клиента tor.exe и прокси-сервера polipo.exe при работе вредоносной программы TorLocker

Для затруднения анализа используются упаковщик UPX (в других программах-шифровальщиках, за исключением CryptoWall, упаковка кода не использовалась) и несколько приемов запутывания кода (так называемая обфускация), что, по замыслу разработчиков этой вредоносной программы, должно было затруднить ее анализ и исследование.

TeslaCrypt (AlphaCrypt) (Trojan-Ransom.Win32.Bitman). Первые образцы этой вредоносной программы появились в ноябре 2014 года (первая загрузка на virustotal.com была зафиксирована 11 ноября 2014 года). За все время своего существования программа претерпела ряд изменений, на данный момент актуальна ее версия TeslaCrypt 2.0.0. Основной вектор заражения этой программы – зараженные наборами эксплойтов Angler EK и Nuclear EK веб-страницы.

Программа выбирает для шифрования порядка 200 типов файлов, при этом последние версии шифруют файлы, относящиеся к некоторым популярным компьютерным играм (файлы с сохраненными пройденными уровнями, пользовательские профили и т.п.) [7, 21].

Реализация шифрования претерпевала изменения от версии к версии. Изначально это был алгоритм AES-256-CBC с сохранением ключа расшифровки в файле key.dat (после зашифровывания последнего файла этот ключ затирался нулями).

В последних версиях (TeslaCrypt 2.0.0) алгоритм шифрования стал более совершенным. По аналогии с вредоносной программой Critroni здесь используется такая же схема шифрования с применением алгоритма шифрования на эллиптических кривых (ECDH) и с сохранением служебной информации в реестре Windows (рис. 22). Все криптографические алгоритмы в этой программе реализованы с помощью свободно распространяемой библиотеки cryptlib, предположительно, версии 3.4.1 [7]. Пример зашифрованного этой программой и исходного файлов показан на рисунке 23 (видно, что объем зашифрованного

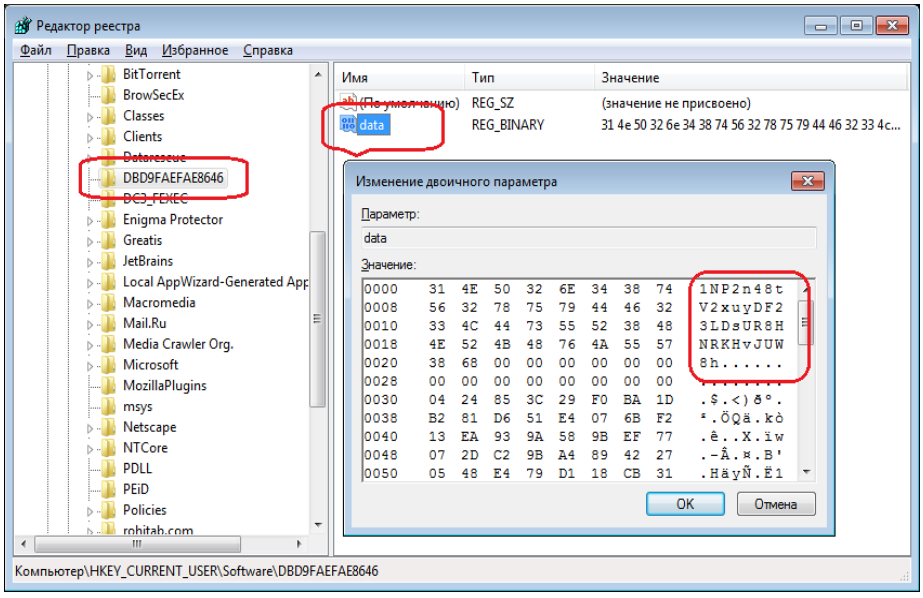

Рис. 22. Служебная информация вредоносной программы TeslaCrypt, сохраненная в реестре

файла за счет добавления служебной информации увеличился на 230 байт).

Перед шифрованием файлов TeslaCrypt с помощью команды vssadmin.exe deleteshadows/all/quiet удаляет все теневые резервные копии системы для исключения возможности восстановления утраченных файлов из этих копий.

Для затруднения анализа зараженной системы вредоносная программа в отдельном потоке, используя API-функции CreateToolhelp32Snapshot, Process32First и Process32Next, ищет процессы с именами taskmgr.exe, regedit.exe, cmd.exe, procexp.exe, msconfig.exe и завершает их.

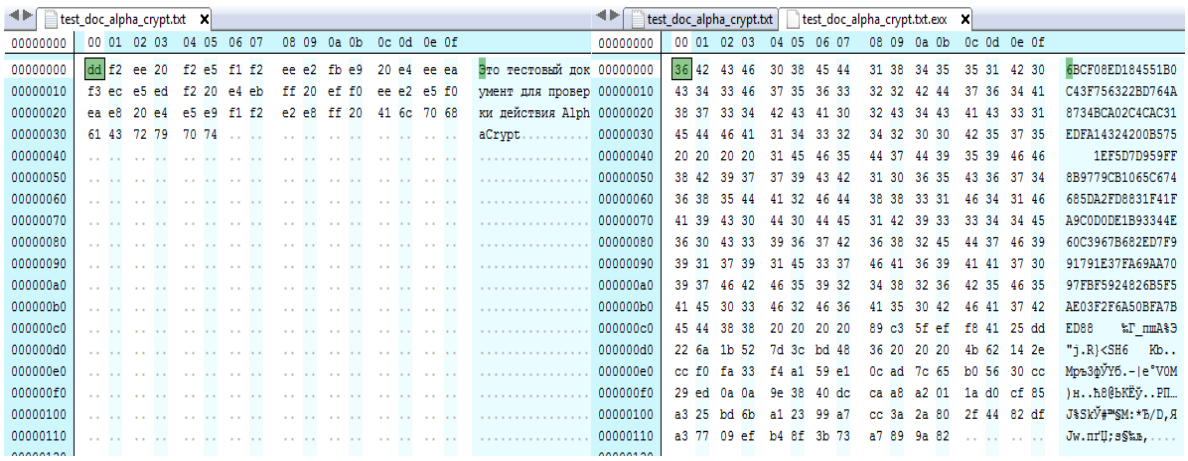

Рис. 23. Незашифрованный (слева) и зашифрованный вредоносной программой TeslaCrypt (справа) файл

В теле программы содержится статический список адресов C&C-серверов. Сами командные серверы находятся в сети tor, но связь с ними осуществляется по протоколу HTTP с помощью tor2web-сервисов (в большинстве образцов этой вредоносной программы используется tor2web.org).

Данная вредоносная программа в ходе своего развития претерпела большое количество усовершенствований. Последние версии этой вредоносной программы используют весьма стойкую схему шифрования с использованием ECDH-алгоритма на эллиптических кривых (по аналогии с вредоносной программой Critroni). Также следует отметить расширение потенциального числа жертв за счет использования любителей компьютерных игр. Для данной категории различные файлы, связанные с играми, представляют большую ценность и многие из них готовы платить выкуп ради восстановления утраченных файлов [22]. TeslaCrypt наряду с вредоносной программой CryptoWall на сегодняшний день активно распространяется, и количество заражений продолжает оставаться довольно высоким.

На основании результатов исследования и анализа этих наиболее распространенных и наиболее характерных образцов вредоносных программ типа «блокиратор-шифровальщик файлов» можно сделать следующие выводы:

- угроза подвергнуться заражению программами данного типа и риску потерять важную информацию по-прежнему актуальна;
- вектор возможных атак вредоносными программами-шифровальщиками сместился от распространения этих программ с помощью спам-рассылок в сторону их распространения с помощью зараженных веб-страниц, что повышает вероятность заражения;
- большинство вредоносных программ этого типа непрерывно совершенствуется, и в самых последних версиях программ такого рода используются весьма стойкие криптографические алгоритмы, не позволяющие расшифровать зашифрованные файлы без знания ключа расшифровки;
- использование для связи с командными центрами анонимных сетей (tor или I2P), а также криптовалюты биткойн в качестве инструмента оплаты выкупа позволяет практически гарантированно обеспечить анонимность злоумышленников и делает очень сложным привлечение их к ответственности;
- применение различных приемов, затрудняющих обнаружение и анализ этих программ, в некоторых случаях позволяет вредоносной программе скрыто осуществлять свою деятельность;
- обнаружение таких вредоносных программ в большинстве случаев возможно только сигнатурным поиском (поскольку выполняемые ими действия характерны не только для вредоносных программ, но и для некоторых других легитимных программ).

Таким образом, основные усилия при борьбе с вредоносными программами такого рода предлагается сосредоточить, во-первых, на создании условий, в которых программа-шифровальщик не сможет осуществлять свою деятельность, во-вторых, на обеспечении резервного копирования критичной информации и обеспечение ее своевременного восстановления из сохраненных копий.

Этого можно достичь за счет следующих мероприятий:

- своевременное обновление антивирусных баз;
- контроль за сетевыми подключениями и разрешение сетевого обмена только ограниченному числу доверенных программ (поскольку некоторые программы-шифровальщики начинают шифрование только после установления связи с командным центром);
- присвоение атрибута «только для чтения» файлам, изменение которых не предусмотрено в процессе работы (фотографии, аудио-, видеозаписи, документы в формате pdf и т.д.);
- организация резервного копирования с использованием какого-либо из средств, не входящих в состав операционной системы (поскольку некоторые вредоносные программы могут удалять теневые резервные копии и точки восстановления системы).

Кроме того, необходима настройка прав доступа к резервным копиям только для программ резервного копирования (для исключения возможного зашифровывания файлов резервных копий), прав доступа к сетевым каталогам и дискам (поскольку многие вредоносные программы могут шифровать файлы на сетевых носителях) и оптимальных параметров системы резервного копирования (период копирования, подлежащие резервному копированию файлы, время хранения резервных копий и т.п.).

Литература

1. Семенченко А. Файлы под «ключ». Эволюция шифровальщиков и ошибки пользователей // Securelist – все об интернет-безопасности. 2015. URL: http://www.securelist.ru/analysis/obzor/25191/fajly-pod-klyuch/ (дата обращения: 21.09.2015).
2. Kaspersky Security Bulletin 2015. Основная статистика за 2015 год. URL: http://www.securelist.ru/files2015/12/KSB_2015_Stats_FINAL_RU.pdf (дата обращения: 15.01.2016).
3. Вредоносная реклама и атаки «нулевого дня»: старые угрозы подрывают доверие к цепочкам поставок и проверенным практикам // Обзор безопасности компании TrendLabs за 1-й квартал 2015 г. TrendMicroIncorporated. URL: http://www.trendmicro.com.ru/media/misc/trendlabs-security-roundup-q1-2015-report-ru.pdf (дата обращения: 21.09.2015).
4. Spam with viruses. URL: http://www.hackmag.com/malware/spam-with-viruses/ (дата обращения: 21.09.2015).
5. Дроботун Е.Б. Обзор свежих эксплойт-паков. Angler, Sweet Orange, Nuclear, Fiesta, Magnitude, Neutrino и многие другие // Хакер. 2015. № 4 (195). С. 78–83.
6. Kotov V., Rajpal M.S. Understanding Crypto-Ransomware // Bromium Labs. December 2014. URL: http://www.bromium.com/sites/defailt/files/bromium-report-ransomware.pdf (дата обращения: 21.09.2015).
7. Дроботун Е.Б. Дети лейтенанта Cryptolocker`a. Вскрываем DirCrypt, TorLocker, TeslaCrypt, TorrentLocker, Critroni и CryptoWall // Хакер. 2015. № 9 (200). С. 206–215.
8. Trojan.Ransomcrypt.D. Technical Details // Symantec. August 2013. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2013-0710112-1247-99&tabid=2 (дата обращения: 21.09.2015).
9. Artenstein N., Shalyt M. How (and why) we defeated DirCrypt // Check Point Malware Research Group. 2014. URL: http://www.checkpoint.com/download/public_files/TCC_WP_Hacking_The_Hacker.pdf (дата обращения: 21.09.2015).
10. Jarvis K. CryptoLocker Ransomware // Dell Secure Works. 2013. URL: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/ (дата обращения: 21.09.2015).
11. Дроботун Е.Б. Анатомия Cryptolocker`a // Хакер. 2014. № 3 (182). С. 102–104.
12. Полиция Массачусетса заплатила выкуп в биткоинах, чтобы вернуть свои файлы. 2014. URL: http://www.geektimes.ru/post/248706/ (дата обращения: 21.09.2015).
13. CryptoWall Ransomware // Dell Secure Works. 2014. URL: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/ (дата обращения: 21.09.2015).
14. Andrea Allievi, Earl Carter. Ransomware on Steroids: Cryptowall 2.0 // Talos Group. 2015. URL: http://www.blogs.cisco.com/security/talos/cryptowall-2/ (дата обращения: 21.09.2015).
15. Синицын Ф. Новое поколение вымогателей. Elliptic curve cryptography + Tor + Bitcoin // Securelist – все об интернет-безопасности. 2015. URL: http://www.securelist.ru/analysis/obzor/21090/novoe-pokolenie-vymogatelej/ (дата обращения: 21.09.2015).
16. CTB-Locker encryption/decryption scheme in details. 2015. URL: http://zarion.wordpress.com/2015/02/17/ctb-locker-encryptiondecription-scheme-in-details/ (дата обращения: 21.09.2015).
17. Marc-Etienne M. Léveillé. TorrentLocker. Ransomware in a country near you // Eset Labs. 2014. URL: http://www.wilivesecurity.com/wp-content/uploads/2014/12/torrent-locker.pdf (дата обращения: 21.09.2015).

18. TorrentLocker – новая модификация трояна-шифровальщика FileCoder. Ч. 1. URL: http://www.habrahabr.ru/company/eset/blog/246945/ (дата обращения: 21.09.2015).

19. TorrentLocker – новая модификация трояна-шифровальщика FileCoder. Ч. 2. URL: http://www.habrahabr.ru/company/eset/blog/247031/ (дата обращения: 21.09.2015).

20. Алюшин В., Синицин Ф. Шифровальщик с изъяном // Securelist – все об интернет-безопасности. 2015. URL: http://www.securelist.ru/blog/issledovaniya/25359/shifrovalshhik-s-izyanom/ (дата обращения: 21.09.2015).

21. TeslaCrypt Ransomware // Dell SecureWorks. 2014. URL: http://www.secureworks.com/cyber-threat-intelligence/threats/teslacrypt-ransomware-threat-analysis/ (дата обращения: 21.09.2015).

22. Синицын Ф. TeslaCrypt 2.0 в обличии CryptoWall // Securelist – все об интернет-безопасности. 2015. URL: http://www.securelist.ru/blog/issledovaniya/26212/teslacrypt-2-0-v-oblichii-cryptowall/ (дата обращения: 21.09.2015).