Шифровирусы шумной толпою... v3.

Уважаемые руководители и сотрудники!

По прежнему (и далее, скорее всего будет еще более) актуальна проблема заражения локальных и сетевых ресурсов шифраторами.

Шифратором является вредоносная программа, которая при запуске в системе скрытно изменяет содержимое документов (doc, docx, xls, xlsx, pdf, jpg, txt и другие) таким образом, что дальнейшая работа с документами становится невозможна.

Основной целью разработчиков шифраторов является вымогательство средств за восстановление или расшифровку документов. При этом используется криптостойкая технология шифрования, при которой зашифрованные файлы не могут быть расшифрованы за разумное время без секретных ключей, которые как правило сохраняются только у злоумышленников.

В настоящее время шифраторы активно распространяются через электронную почту, реже через веб-страницы.

Как правило, действует целая команда мошенников: одни пишут программы, другие собирают электронную почту пользователей, для последующих целевых атак,
третьи изучают целевые группы пользователей и готовят тексты электронных писем с использованием методов соц_инженерии, четвертые размещают архивы программ с шифраторами на удаленных серверах.

Цель соц_инженеров заключается в том, чтобы создать ситуацию, в которой пользователь получив электронное сообщение начинает действовать строго по указанию инженеров, забывая об элементарных принципах безопасности.

В ход идут уловки: "выгодное предложение", "просьбы о спасении", "судебные риски" с предложением действовать как можно быстрее, сейчас, срочно, иначе будет причинен какой то ущерб (неполучение прибыли, штрафа, санкции и т.п.)

Письмо, составленное по всем правилам соц_инженерии, на первый взгляд будто действительно адресовано Вам и от доверенного (или известного) адресата.

Темы писем могут быть с таким содержанием:
"ознакомьтесь с архивом документации по судебному иску в качестве свидетеля по делу....", "резюме"
и т.п.

Добрый день!

К нам заявились налоговики с проверкой((
Мы уже второй день пытаемся найти некоторые первичные документы, касающиеся нашего сотрудничества.
Но в связи с переездом в новый офис, акты и несколько договоров между нами так и не были найдены.
Я составила список документов (во вложении). Прошу Вас помочь с их поиском...
Скиньте хотя бы скан-копии, а то мы влетим на штрафы.
Заранее большое спасибо!

Прикреплённые файлы:
<u>1. Список документов.zip</u>

--
С Уважением
Сотрудники бухгалтерии
ООО "Город Инструмента"

Уважаемые коллеги,
Пересылаю счета-фактуры согласно Договора от 22.10.2014 года (во вложении).
Пожалуйста, погасите неоплаченный остаток за пользование системой "Консультант Плюс". Средства в полном объеме мы так и не получили, хотя прошло уже больше 2 месяцев..
По нашей оборотно-сальдовой ведомости за вами числиться небольшой долг.
Если оплата не будет произведена в ближайшие 10 дней, мы будем вынуждены прекратить Ваше обслуживание.

Спасибо.

ПРИКРЕПЛЁННЫЕ ФАЙЛЫ:
1. Счета.zip [1]

--
С Уважением,
Алина Островская
Старший менеджер по работе с клиентами
КонсультантПлюс

День добрый,
В связи с кризисом наше руководство было вынуждено несколько пересмотреть цены.
Просьба ознакомиться с исправленными счетами и сообщить о возможности доплаты.
Очень надеемся на Ваше понимание.
Благодарим.

--
ООО "ПРОМИНДУСТРИЯ"
тел: 8 (495) 783-01-02

Электронное сообщение, как правило, содержит документ, вложенный архив (rar,zip реже 7z) или ссылку на архив из сети.

например:
Архивная документация о привлечении в качестве свидетеля по гражданскому делу №233669.zip
Счета-фактуры номер 19212-15 19217-15 для проведения оплаты и погашения задолженности _ согласовано doc.zip
Перерасчет по итогам первого квартала 2015 года.rar

В архиве, как правило содержится документ с длинным наименованием и видимой иконкой (соответствует doc, pdf, xls и др).

Имя вложенного документа формируется таким образом, чтобы пользователь не видел конечное расширение файла, т.е. после видимого doc, xls, pdf может быть множество пробелов и конечное расширение на самом деле может быть: .bat, .cmd, .exe, .com, .js, .hta, .pif, .scr

Обратите внимание, что файлы с данным расширением .bat, .cmd,.exe, .com, .js, .hta, .pif, .scr являются исполняемыми программами, и никак не могут быть нормальными офисными документами или рисунками, которые чаще всего и присутствуют в электронном обороте.

Если вам предлагают открыть исполняемый файл с данным расширением, выдавая его за офисный документ, то это очевидное мошенничество с целью выдать черное за белое.

Если в письме добавлена ссылка на файл, (который необходимо выкачать из сети), наведите курсор мыши на ссылку (не нажимая кнопок), по которой вам предлагают скачать архив с документами.
Обратите внимание, с какого адреса вам предлагают скачать данных файл.

если используются подобные адреса, то это верный признак того, что вам хотят "впарить" документ сомнительного содержания:

2theloo.co
anglersparadise.info
askbasim.com
biz-sales.net
celiklerkuruyemis.com
chanasociety.com
creative-metal.lv
hellobit.co
hukport.com
integraled.com
integres.com
jimail.ru
kimail.ru
llmaill.ru
mbellrealty.com
meetfeli.net
mercer-designs.com
oruzhkov.net
polybutylenecarolina.com
procyanide.com
qyzc8.com
subqmail.com
twitterkeybtc.com
unibk.com
vanderputten.fr
xn--e1aji5e.xn--p1ai
xn--e1aji5e.xn--p1ai/
янке.рф
янке.рф/
attach*.com*
attached-email.com*
deesidescouts*.org.uk*
download-attach.com*
jordinas.com*
letter-attachment.com*

В последнее время появились новые варианты запуска шифраторов:
в электронное сообщение может быть добавлен офисный документ doc,docx, xls, xlsx (в архиве или без архива)

При открытии данного документа пользователю может быть предложено изменить настройки безопасности защиты от макровирусов до среднего или низкого уровня.
Или запустить внедренный объект, замаскированный под видом анкеты в формате pdf или презентации.

Подобные документы необходимо сразу закрыть и удалить. А электронное сообщение отправить в спам или в удаленные.

От ваших корреспондентов необходимо запрашивать корректные документы (по возможности с цифровой подписью) без всяких внедренных объектов и макросов.

В случае, если такой документ будет открыт вами, и при этом обойдены антивирусная защита и политики ограниченного запуска программ запускается исполняемая программа, которая выкачивает из сети необходимые файлы и запускает процесс шифрования ваших документов.
При этом шифруются документы (doc, docx, xls, xlsx, pdf, jpg, и др.) на вашем персональном компьютере, а так же на всех сетевых и съемных дисках, которые будут подключены в данный момент.

Внешние признаки запуска шифратора:
Резко снизилась производительность компьютера, медленно открываются документы с сетевых дисков, стали меняться иконки документов на рабочем столе, имена и расширения документов:

Договор купли-продажи автомобиля.doc.vault
ydyGIxO-c8A (1).jpg.keybtc@gmail_com
Приложение№1 АЛАДИН.docx.keybtc@gmail_com
Госзадание на 201-2015 учебный год.pdf.paycrypt@gmail_com
readme.TXT.ykjdruh
email-eric.decoder10@gmail.com.ver-CL 1.1.0.0.id-TBHMTZDJPVAFLRWCHNSYEJOUAFKQWBHMSYDI-06.08.2015 14@39@447462257.randomname-AHNAGMSXDJPUAGLRXDINTZEKQVBHNS.ZFJ.cbf
email-eric.decoder10@gmail.com.ver-CL 1.1.0.0.id-TBHMTZDJPVAFLRWCHNSYEJOUAFKQWBHMSYDI-06.08.2015 14@39@447462257.randomname-IPVAHNRXDJOTZFKPVBGLRXCHNTYDJP.VAG.cbf
email-Seven_Legion2@aol.com.ver-CL 1.1.0.0.id-BCDDEFGHHIJJKLMMNNOPQQQRSTUVVVWXYYZZ-04.08.2015 9@15@456982965.randomname-GHIIJKLLMNOOOPQRSSSTUVWWWXYZZA.BBC.cbf
Сигнатуры вирусов.txt.id-9910836847_support@recovery
Алмаз-Антей.doc.id-4701762356_blockchain@inbox.com
Совещание от 26.09.2014г.rtf.id-9753984971_maxcrypt@foxmail2.com
Правила поведения вахтеров.jpg.id-2561608692_sos@xsmail.com
Инструкция по партнерам.doc.just
BHeEjlz4GxA+iW7IzEYHCLfN8vX6-2bpPwFXfxv6jM1mRgfjDYF976bMRcA0qGqB.xtbl
aRSk9EyQ5oC7wgMoCQvsyUAB+-CaF+nAlHZxEG3ElS0E9xnccTXvmMUhxRMUJkE94OlFsVyVVSnRs1TDuQ+I2oUozqRcZiZdLngSUr-uNnc=.xtbl
Письмо Амуршина бг.doc.-.DIRECTORAT1C@GMAIL.COM.roto
15092014 16_55_03.xls.backyourfiles@126.com_Ief3M

В этом случае необходимо сразу выключить компьютер и сообщить об инциденте администратору. В дальнейшем без санкции администратора компьютер не включать.

Чтобы данный процесс не случился на вашем компьютере, обратите внимание на следующие моменты:

1. на вашем компьютере обязательно должен быть установлен антивирус.
(если не установлен антивирус - сообщите в вашу техническую поддержку или администратору.)

2. антивирус должен быть в актуальном состоянии, с регулярным обновлением антивирусных баз;

3. желательно, чтобы ваши браузеры и почтовые клиенты были обновлены до актуальных версий. (за исключением, если вы работаете с Internet Explorer, настроенным на работу с тендерными площадками, или онлайн банком.)

4. Если электронное сообщение явно не адресовано вам – не открывайте его.

5. Часто электронное сообщение содержит в архиве лишь небольшой загрузчик шифратора размеров несколько кб. Если вы распаковали файл из архива на рабочий стол, или в отдельный каталог, обратите внимание на расширение данного документа. Документы с расширением .bat, .cmd,.exe, .com, .js, .hta, .pif, .scr отправляем сразу в корзину.

5. Не пересылайте сообщение с подобными архивами вашим коллегам с просьбой посмотреть что там за вложение, которое не открывается на вашем компьютере. (получится, что сами запустили шифратор, и передали его коллегам, но уже с вашего доверенного адреса – коллеги, естественно сделают то же, что уже сделали вы – в итоге имеем массовое заражение.)

6. перешлите подозрительное сообщение для проверки администратору.

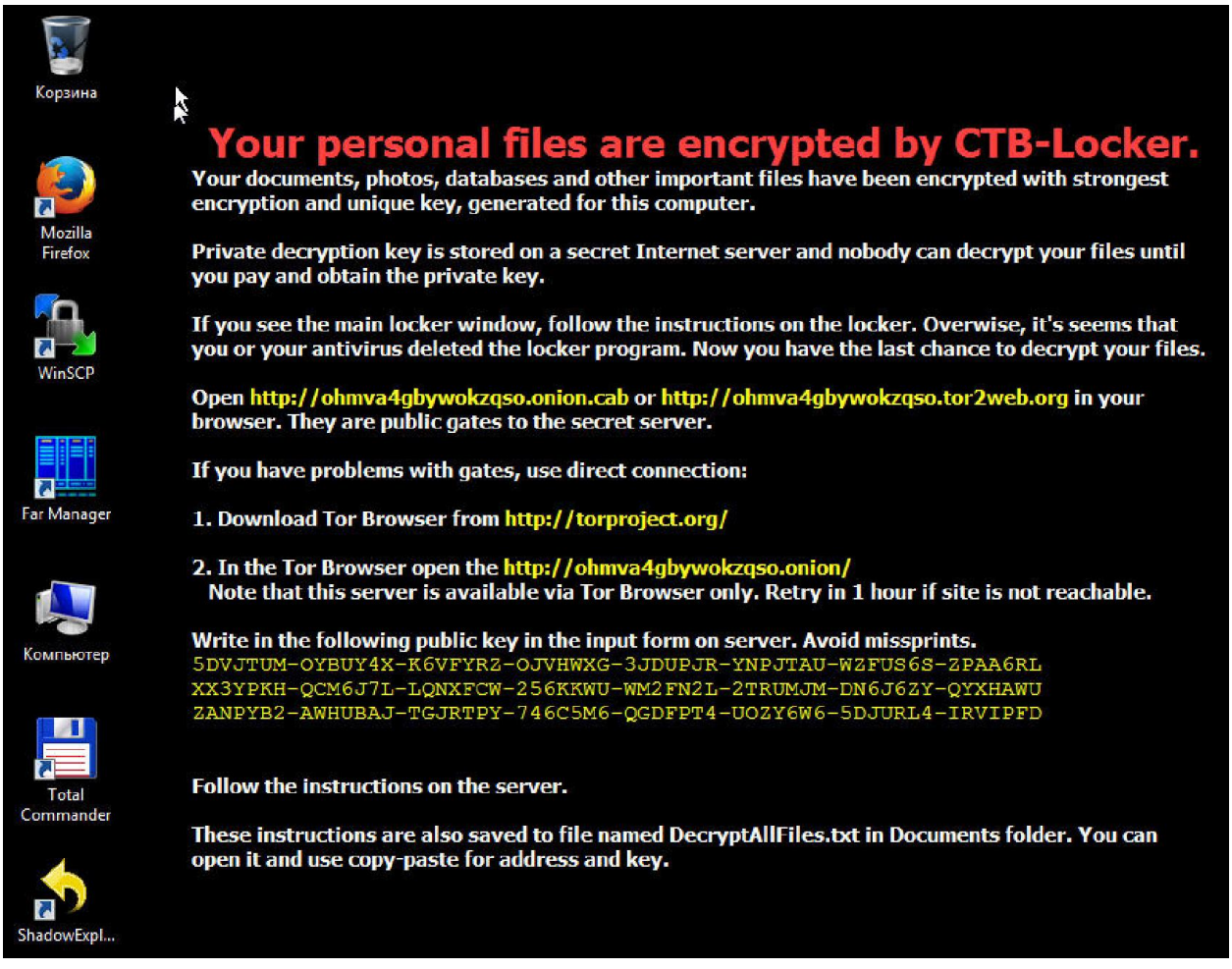
7. не забываем классику. (песенку персонажей Алисы и Базилио из "Приключения Буратино")

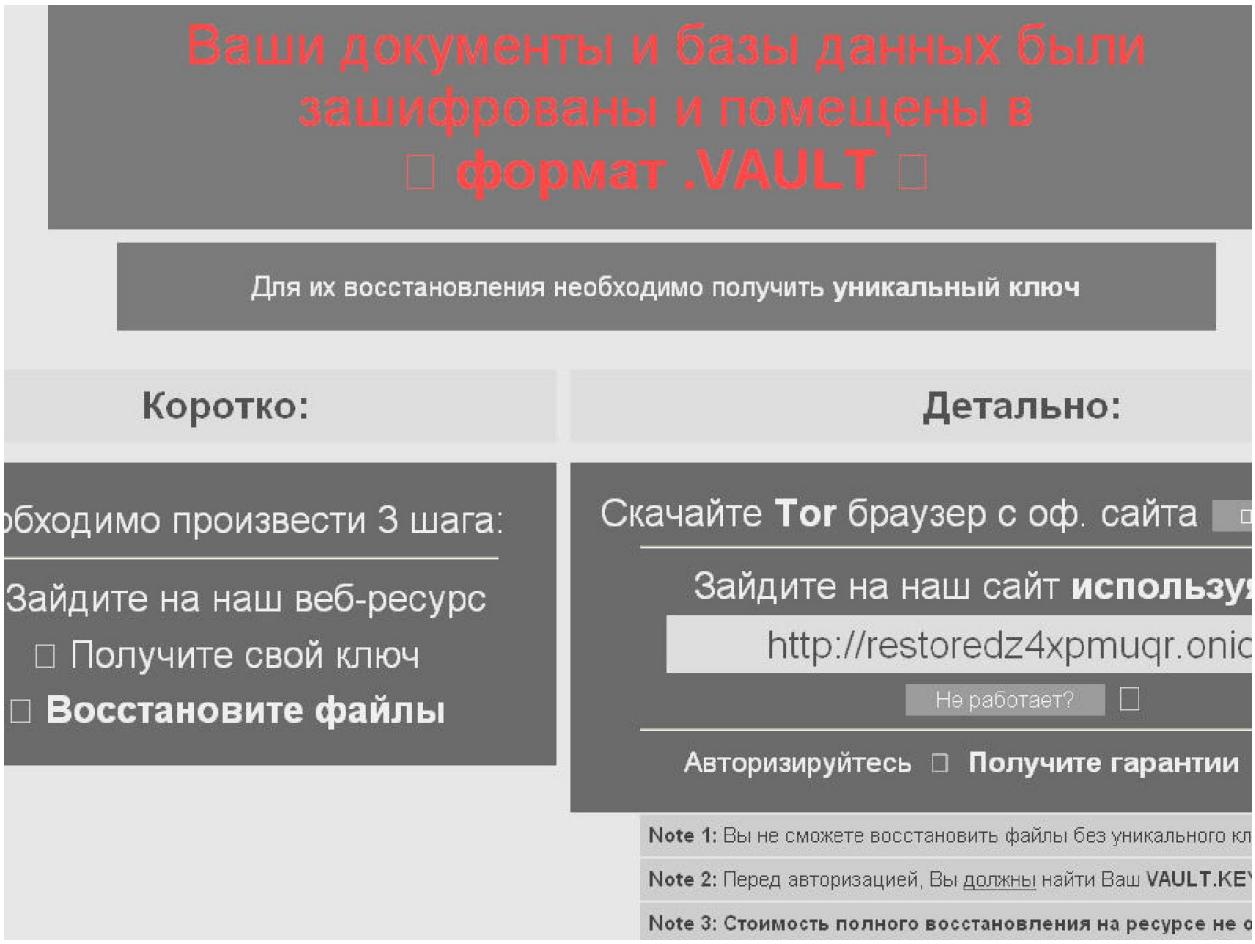
Итого:

8. документы зашифрованные (подобными методами) скорее всего не получится расшифровать. Если не будет копий ваших документов, Вы можете потерять результаты вашей работы в течение нескольких лет.

9. Если Вы обнаружили, что ваши файлы не открываются и имеют странное и длинное расширение, то самое опасное уже произошло, и процесс шифрования запущен. (а может быть уже завершен)
В этом случае, необходимо сразу **выключить компьютер, сообщить об этом (инциденте) администраторам. и ждать проверки вашей системы.**

Так выглядит победа мошенников над нашей доверчивостью, невнимательностью, незнанием правил безопасной работы в сети:





Внимание !

Если Вы читаете это сообщение, значит Ваш компьютер был атакован опаснейшим вирусом.Вся Ваша информация (документы, базы данных, бэкапы и другие файлы) на этом компьютере была зашифрована.

Все зашифрованые файлы имеют расширение protectdata@inbox.com

Ни в коем случае не изменяйте файлы!

И не используйте чужие дешифраторы,

Вы можете потерять Ваши файлы навсегда.

Стоимость дешифра 200 $

Напишите письмо на адрес protectdata@inbox.com , чтобы узнать как получить дешифратор.

Если мы Вам не ответили в течении 3 часов

- повторите пересылку письма на protectdata@inbox.com

Через 48 часов ваш пароль будет удалён из базы.

В первом письме не прикрепляйте файлы для дешифровки.

Все инструкции вы получите в ответном письме.