ProLock

id-ransomware.blogspot.com/2020/03/prolock-ransomware.html

ProLock Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью AES+RSA, а затем требует выкуп от 35 до 255 BTC, чтобы вернуть файлы. Оригинальное название: ProLock (указано в записке).

Важно! Оригинальный дешифровщик из-за ошибки не может расшифровать файлы размером более 64 Мб, поэтому уплата выкупа в этом случае бесполезна. Возможно это будет исправлено позже, но если вы решили заплатить выкуп, требуйте подтверждения, что файлы более 64-100 Мб будут корректно расшифрованы. **Вы можете заказать расшифровку в Emsisoft по ссылке >>** .

Обнаружения:
DrWeb -> Trojan.Packed2.42421, Trojan.Encoder.32444
BitDefender -> Trojan.GenericKD.42886619
Kaspersky -> Trojan-Ransom.Win32.Pwnd.c
Qihoo-360 -> Win32/Trojan.Ransom.7de
Tencent -> Win32.Trojan.Pwnd.Sxxx
TrendMicro -> Ransom.Win32.PROLOCK.AA

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: PwndLocker > ProLock

Изображение — логотип статьи

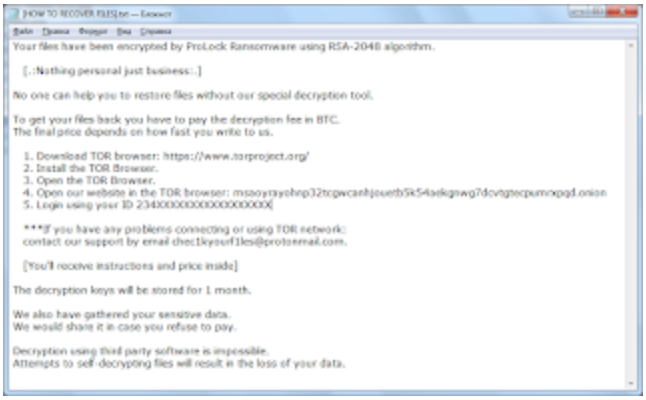
К зашифрованным файлам добавляется расширение: **.ProLock**

Также используются вариации:
.proLock
.pr0Lock
.proL0ck

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на середину марта 2020 г. Предыдущий вариант вымогателя, который был назван **PwndLocker**, имел уязвимость, позволявшую расшифровать файлы у некоторых пострадавших, поэтому был модифицирован злоумышленниками с учетом имевшей уязвимости. ProLock ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Только в США он нацелен на организации в следующих секторах: здравоохранение, правительство, финансы и розничная торговля.

Записка с требованием выкупа называется: **[HOW TO RECOVER FILES].txt**


[HOW TO RECOVER FILES].txt — Блокнот

Файл Правка Формат Вид Справка

Your files have been encrypted by ProLock Ransomware using RSA-2048 algorithm.

[..:Nothing personal just business:..]

No one can help you to restore files without our special decryption tool.

To get your files back you have to pay the decryption fee in BTC.
The final price depends on how fast you write to us.

1. Download TOR browser: https://www.torproject.org/
2. Install the TOR Browser.
3. Open the TOR Browser.
4. Open our website in the TOR browser: msaoyrayohnp32tcgwcanhjouerb5k54adkgnwg7dcvngtecpumxpqd.onion
5. Login using your ID 234XXXXXXXXXXXXXXXX

***If you have any problems connecting or using TOR network:
contact our support by email chectkyourfiles@protonmail.com.

[You'll receive instructions and price inside]

The decryption keys will be stored for 1 month.

We also have gathered your sensitive data.
We would share it in case you refuse to pay.

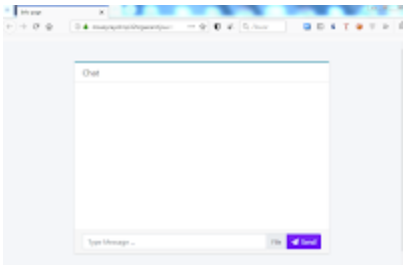
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.

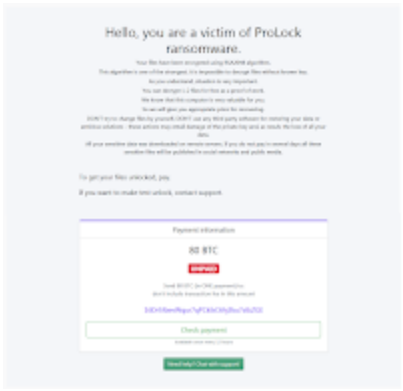
Содержание записки о выкупе:
Your files have been encrypted by ProLock Ransomware using RSA-2048 algorithm.

[.:Nothing personal just business:.]
No one can help you to restore files without our special decryption tool.
To get your files back you have to pay the decryption fee in BTC.
The final price depends on how fast you write to us.
1. Download TOR browser: https://www.torproject.org/
2. Install the TOR Browser.
3. Open the TOR Browser.
4. Open our website in the TOR browser:
msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion
5. Login using your ID 234********** [total 20 characters]
***If you have any problems connecting or using TOR network:
contact our support by email chec1kyourf1les@protonmail.com.
[You'll receive instructions and price inside]
The decryption keys will be stored for 1 month.
We also have gathered your sensitive data.
We would share it in case you refuse to pay.
Decryption using third party software is impossible.
Attempts to self-decrypting files will result in the loss of your data.

Перевод записки на русский язык:
Ваши файлы зашифрованы ProLock Ransomware с использованием алгоритма RSA-2048.
[.:Ничего личного просто бизнес:.]
Никто не может помочь вам восстановить файлы без нашего специального инструмента расшифровки.
Чтобы вернуть ваши файлы, вы должны заплатить за расшифровку в BTC.
Окончательная цена зависит от того, как быстро вы напишите нам.
1. Загрузите браузер TOR: https://www.torproject.org/
2. Установите браузер TOR.
3. Откройте браузер TOR.
4. Откройте наш веб-сайт в браузере TOR:
msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion
5. Войдите под своим ID 234********** [всего 20 символов]
*** Если у вас есть проблемы с подключением или с сетью TOR:
свяжитесь с нашей службой поддержки по email chec1kyourf1les@protonmail.com.
[Вы получите инструкции и цену внутри]
Ключи расшифровки будут храниться в течение 1 месяца.
Мы также собрали ваши конфиденциальные данные.
Мы поделимся этим, если вы откажетесь платить.
Расшифровка с использованием сторонних программ невозможна.
Попытки самостоятельно расшифровать файлы приведут к потере ваших данных.

Скриншоты сайта вымогателей:





Содержание текста на сайте вымогателей:
Hello, you are a victim of ProLock ransomware.
Your files have been encrypted using RSA2048 algorithm.
This algorithm is one of the strongest, it is impossible to decrypt files without known key.
As you understand, situation is very important.
You can decrypt 1-2 files for free as a proof of work.
We know that this computer is very valuable for you.
So we will give you appropriate price for recovering.
DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - these actions may entail damage of the private key and, as result, the loss of all your data.
All your sensitive data was downloaded on remote servers. If you do not pay in several days all these sensitive files will be published in social networks and public media.
To get your files unlocked, pay.
If you want to make test unlock, contact support.
Payment information
80 BTC
UNPAID
Send 80 BTC (in ONE payment) to:
don't include transaction fee in this amount
16Dr9JbevWqur7qPCkfxC6hj3ku7stbZGE
[Check payment]
Available once every 12 hours
[Need help? Chat with support!]

Перевод текста на русский язык:
Привет, вы жертва ProLock Ransomware.
Ваши файлы зашифрованы с использованием алгоритма RSA2048.
Этот алгоритм является одним из самых сильных, невозможно расшифровать файлы без известного ключа.
Как вы понимаете, ситуация очень важна.
Вы можете расшифровать 1-2 файла бесплатно как доказательство работы.
Мы знаем, что этот компьютер очень ценен для вас.
Поэтому мы дадим вам соответствующую цену для восстановления.
НЕ ПЫТАЙТЕСЬ изменить файлы самостоятельно, НЕ ИСПОЛЬЗУЙТЕ какую-то стороннюю программу для восстановления ваших данных или антивирусные решения - эти действия могут повлечь за собой повреждение личного ключа и, как следствие, потерю всех ваших данных.
Все ваши конфиденциальные данные были загружены на удаленные серверы. Если вы не заплатите в течение нескольких дней, все эти конфиденциальные файлы будут опубликованы в социальных сетях и общедоступных СМИ.
Чтобы получить доступ к файлам, заплатите.
Если вы хотите сделать тест-разблокировку, обратитесь в службу поддержки.
Платежная информация
80 BTC
НЕОПЛАЧЕНО
Отправьте 80 BTC (ОДИН платеж) на:
не включайте комиссию за транзакцию в эту сумму
16Dr9JbevWqur7qPCkfxC6hj3ku7stbZGE
[Проверить оплату]
Доступно раз в 12 часов
[Нужна помощь? Общайтесь за поддержкой!]

Технические детали

Для распространения используется **QakBot** (Qbot, банковский троян, распространяющийся с помощью фишинговых кампаний, email-спама и и вложенных вредоносных документов Microsoft Word). Ранее QakBot был связан с MegaCortex. QakBot загружает пакетные сценарии из облачного хранилища и выполняет их с помощью команды:

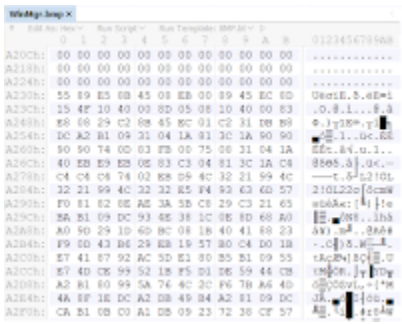
```
schtasks.exe /CREATE /XML C:\Programdata\WinMgr.xml /tn WinMgr
schtasks.exe /RUN /tn WinMgr
del C:\Programdata\WinMgr.xml

del C:\Programdata\run.bat
```

ProLock крадет данные из скомпрометированной сети. Для эксфильтрации файлы архивируются с помощью архиватора 7-zip и загружаются в облачные хранилища (OneDrive, Google Drive, Mega) с помощью программы командной строки **Rclone**, которая синхронизирует данные с большим количеством облачных хранилищ. После эксфильтрации операторы выполняют сценарий PowerShell, чтобы извлечь двоичный файл ProLock, встроенный в файл образа, и развернуть его в корпоративной сети для шифрования данных в достижимых системах.

Кроме того, ProLock может распространяться путём взлома через незащищенную конфигурацию RDP со слабыми паролями, с помощью обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

➤ ProLock использует PowerShell для внедрения в память специального файла WinMgr.bmp. Файл в заголовке является файлом BMP или JPG, за которым идут нули, а затем код вымогателя.



Вы можете видеть это на скриншотах. Файл WinMgr.bmp при просмотре выглядит как чёрный фон с несколькими белыми точками в правом верхнем углу. Его анализ на сайте VT приложен ниже.
Если посмотреть на файл в hex-редакторе, то можно увидеть, что он содержит встроенные в него двоичные данные. Именно эти двоичные данные считываются PowerShell-скриптом, который внедряет их в память.

Такая атака возможна при открытом доступе к серверам предприятия или организации с помощью службы удаленного рабочего стола. Далее развертывании по всей сети осуществляется с использованием PowerShell Empire или PSExec.

➤ ProLock удаляет теневые копии файлов командами:
vssadmin.exe delete shadows /all /quiet
vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=401MB
vssadmin.exe resize shadowstorage /for=D: /on=D: /maxsize=unbounded

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
[HOW TO RECOVER FILES].txt - название файла с требованием выкупа
WinMgr.bmp - чёрный файл с белыми точками и кодом вымогателя внутри.
WinMgr.xml
run.bat
clean.bat
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\ProgramData\WinMgr.bmp
C:\Programdata\WinMgr.xml
C:\Programdata\clean.bat
C:\Programdata\run.bat

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion
Email: chec1kyourf1les@protonmail.com
BTC: 16Dr9JbevWqur7qPCkfxC6hj3ku7stbZGE
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ **VirusTotal analysis (WinMgr.bmp) >>**
🐞 Intezer analysis >>
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ **JOE Sandbox analysis >>**

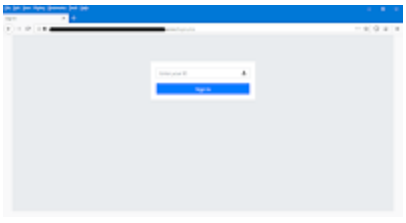
Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

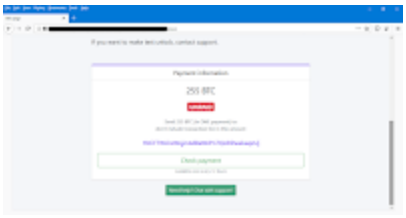
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 14-18 мая 2020:
Статья на сайте Group-IB >>
Статья на сайте BleepingComputer >>
2-я статья на сайте BleepingComputer >>

Обновление от 28 августа 2020:
Пост в Твиттере >>
Расширение: **.pr0Lock**
Записка: [HOW TO RECOVER FILES].TXT
Email: chec1kyourf1les@protonmail.com
Результаты анализов: **VT + AR**

Обновление от 10 сентября 2020:
Статья от Group-IB (in English) >>
Русская версия статьи >>

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===

Вы можете заказать индивидуальную расшифровку в Emsisoft.

Для этой перейдите на сайт Emsisoft по ссылке >>

Read to links:

+ Tweet + **myTweet**
ID Ransomware (ID as ProLock)
Write-up (March 20, 2020), Topic of Support
*

Thanks:

PeterM, Michael Gillespie
Andrew Ivanov (author)
Lawrence Abrams
to the victims who sent the samples