XiaoBa

Archived: 2026-04-05 18:38:07 UTC

XiaoBa Ransomware

(шифровальщик-вымогатель, деструктор)

Этот крипто-вымогатель шифрует данные пользователей с помощью AES/RSA, а затем требует выкуп в 1200 юаней = 180,81$ в BTC, чтобы вернуть файлы. Оригинальное название: XiaoBa. На файле написано: xiaoba.exe. Написан на языке FlyStudio.

© Генеалогия: XiaoBa > XiaoBa 2.0

К зашифрованным файлам добавляются расширения от **.XiaoBa1** до **.XiaoBa34**

Активность этого крипто-вымогателя пришлась на вторую половину октября 2017 г. Ориентирован на китайских пользователей, что не мешает распространять его по всему миру.

Записки с требованием выкупа называются:
@XiaoBa@.bmp
@Explanation@.hta

Содержание записки о выкупе:
Ooops, your important files have been encrypted!
！------ 重要加密 ------ ！
你柏所有文件已被 RSA-2048 AES-128 算法進行了加密
請硕縱破解 ，因為您無 眷破解文件可能導致文壞 這可能會損害他們

只有我們的解密辦捕解密您的文件
如果您看到這個壁紙卻看不到 “XiaoBa” 窗口 , 那麼就是您的防病毒軟件
刪除了此解密軟件或葡恣從計算機中刪除了它
如果您需要您的文件I必須運行解密軟件
請找到解密軟件或從防病毒軟件隔雜區還原
運行解密軟件 , 並按照說明進行操作
請向指定地址發送約1200元人民幣=180.81$的比特幣
比特幣錢包：1GoD72v5gDyWxgPuBph7zQwvR6bFZyZnrB
想獲取更多信息請點擊桌面的 _@Explanation@_.hta
E-mail:B32588601@163.com

Перевод записки на русский язык:
Упс, все ваши важные файлы зашифрованы!
！------ Важные файлы зашифрованы ------ ！
Все файлы зашифрованы с алгоритмами RSA-2048 AES-128
Попробуйте взломать, но вы не вернете файлы, это приведет к тому, что текст может быть повреждён.
Только наше дешифрование может вернуть ваши файлы.
Если вы видите эти обои, но не видите окно "XiaoBa", то ваша антивирусная программа поместила эту программу в карантин или удалила с компьютера.
Если вам нужны файлы, то вы должны заново запустить нашу программу для дешифрования.
Найдите нашу программу для дешифрования или восстановите её из карантина антивируса.
Запустите программу дешифрования и следуйте инструкциям.
Пожалуйста, отправьте около 1200 юаней = 180,81$ в биткоинах на указанный адрес BTC-кошелька: 1GoD72v5gDyWxgPuBph7zQwvR6bFZyZnrB
Для получения информации найдите на рабочем столе файл _@Explanation@_.hta
E-mail: B32588601@163.com

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, эксплойтов, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

➤ Создает множество процессов.

➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки, удаляет точки восстановления командой:
cmd /c vssadmin delete shadow /all /quiet & wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

➤ Зашифрованные файлы повреждаются. **Уплата выкупа бесполезна!**

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:
@XiaoBa@.bmp
@Explanation@.hta
xiaoba.exe
AutoRunApp.vbs

Расположения:
\Desktop_@Explanation@_.hta
C:\AutoRunApp.vbs

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

Сетевые подключения и связи:
URL: http://baidu.com
http://tieba.baidu.com
http://wenku.baidu.com
http://xueshu.baidu.com
http://zhidao.baidu.com и другие
Email: B32588601@163.com
BTC: 1GoD72v5gDyWxgPuBph7zQwvR6bFZyZnrB
См. ниже результаты анализов.

Результаты анализов:
Гибридный анализ >>
VirusTotal анализ >> VT+
Другой анализ >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно.

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

Обновление от 4 ноября 2017:

Сумма выкупа: 250 RMB (китайские юани) = $37.696 в BTC

Email: B32588601@163.com

BTC: 1NodpehhyEnJZUE3vsGXHm8RYLfydMZkv4

Экран пользователь блокируется.

Результаты анализов: HA+ VT

<< Скриншот с требованиями выкупа

Обновление от 18 ноября 2017:

Пост в Твиттере >>

Сумма выкупа: 0.1 BTC

Email: TheYuCheng@yeah.net

BTC: 17SGfA1QSffaDMnG3TXEC4EiLudjLznQR6

Результаты анализов: VT

<< Скриншот с требованиями выкупа

См. статью Want Money Ransomware >>

Обновление от 24-27 февраля 2018:

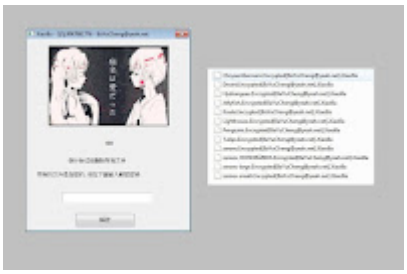
Пост в Твиттере >> + Tweet

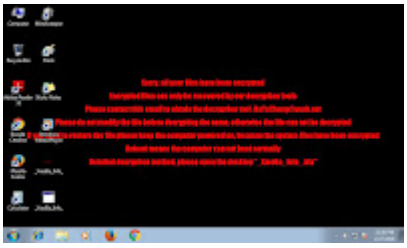
Расширение: .Encrypted[BaYuCheng@yeah.net].XiaBa

Записка: _XiaoBa_Info_.hta

Email: BaYuCheng@yeah.net

Результаты анализов: VB + VT + VT

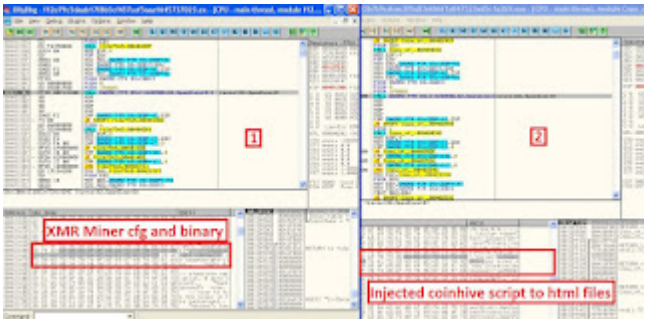


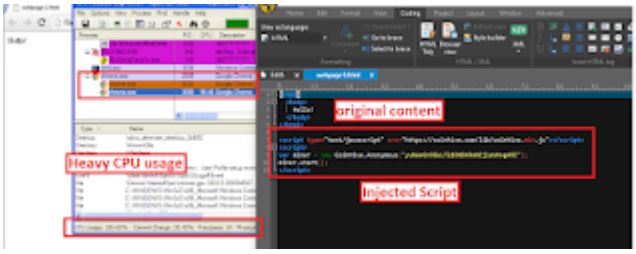


Обновление от 17 апреля 2018:

➤ Теперь XiaoBa присоединяет майнер coinminer к исполняемым файлам (.exe, .com, .scr, .pif) на всём жестком диске, включая основные папки операционной системы. После этого запуск любого из заряженных таким образом исполняемых файлов запускает только coinminer, а не само приложение. Это приводит к проблемам, при которых Windows не сможет загрузиться.

➤ XiaoBa также внедряет (инжектирует) скрипт Coinhive во все файлы HTML и HTM, а также удаляет все файлы с расширениями .gho и .iso, которые часто используются в антивирусных образах Live-CD/DVD (например, Norton Ghost использует файлы с расширением .gho, а Kaspersky Rescue Disk использует .iso).





➤ Другой вариант XiaoBa тоже инжектирован, но также содержит 32-битную и 64-битную версию майнера XMRig.

Подробности в **статье** от TrendMicro.

Обновление от 5 июня 2018:

Пост в Твиттере >>

Расширение: .AdolfHitler
Email: BaYuCheng@yeah.net
Записка-изображение: # # DECRYPT MY FILE # #.bmp
Файл: New Folder.exe
Результаты анализов: VT

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

Read to links:
Tweet on Twitter
ID Ransomware (ID as XiaoBa)
Write-up, Topic of Support
*

Thanks:
MalwareHunterTeam
Michael Gillespie
*
*
