

MBRlock, Hax

Archived: 2026-04-05 18:57:46 UTC

MBRlock Ransomware

Aliases: Haxlocker, Dexcrypt

(шифровальщик-вымогатель, MBR-модификатор)

Этот крипто-вымогатель шифрует диски пользователей, а затем требует выкуп в 30 юаней, чтобы вернуть файлы. Оригинальное название: **MBRlock** и **Hax**. Китайское название: 易语言程序. На файле написано: Hax.exe. Написан на языке FlyStudio. В обновлениях также могут быть неродственные варианты.

Обнаружения:

DrWeb -> Trojan.MBRlock.280

ALYac -> Trojan.Ransom.MBRLOCK

Avira (no cloud) -> TR/Ransom.MBRlock.qqmpg

BitDefender -> Gen:Variant.Ransom.MBRLOCK.3

ESET-NOD32 -> Win32/MBRlock.AZ

Malwarebytes -> Trojan.MalPack.FlyStudio

Microsoft -> Ransom:Win32/Dexcrypt

Rising -> Ransom.Dexcrypt!1.B151 (CLASSIC)

TrendMicro -> Ransom_HAXLOCKER.THBIBH

© Генеалогия: выясняется.

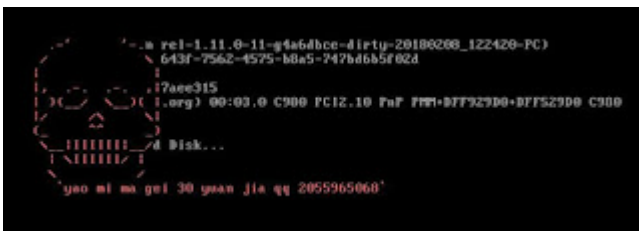


Изображение робота на иконке файла Нах.exe

К зашифрованным файлам добавляется расширение *нет данных*.

Активность этого крипто-вымогателя пришлась на начало февраля 2018 г. Ориентирован на китайских и англоязычных пользователей, что не мешает распространять его по всему миру.

Запиской с требованием выкупа выступает чёрный экран блокировки:



Скриншоты разных образцов имеют различия в тексте

Содержание записки о выкупе:

Your disk have a lock!!!Please enter the unlock password
уао ми ма геи 30 yuan jia qq 2055965068

Перевод записки на русский язык:

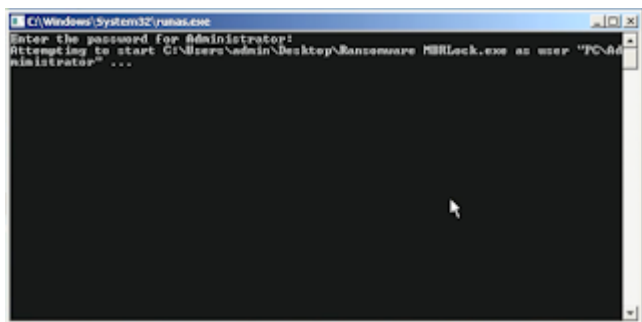
На вашем диске замок!!! Введите пароль разблокировки
Пароль за 30 юаней на qq 2055965068

Технические детали

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

!!! 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](#).

- После установки MBRLocker сразу перезагружает компьютер, а жертве показывается чёрный экран с изображением черепа в ASCII и сообщением отправить 30 юаней на адрес qq 2055965068, чтобы вернуть доступ к компьютеру.
- Требуется права администратора на блокировку MBR. Получив права перезаписывает MBR.



- 👉 Восстановить доступ можно стандартными средствами восстановления Windows: fixmbr и fixboot.
- 👉 Предварительно защитить диск можно с помощью бесплатного инструмента [MBRFilter](#).

Список файловых расширений, подвергающихся шифрованию:

.BMP, .CUR, .GIF, .ICO, .JPG, .MID, .PNG, .prn, .txt, .WAV (10 расширений).

Это текстовые файлы, фотографии, музыка, иконки, курсоры и пр.

Файлы, связанные с этим Ransomware:

Ransomware MBRLock.exe (Hax.exe)

runas.exe

<random>.exe

360.dll и другие

► Судя по результатам анализа, использует файлы от китайского антивируса 360 Security.

Расположения:

\Desktop\Ransomware MBRLock.exe

C:\Windows\System32\runas.exe

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Сетевые подключения и связи:

См. ниже результаты анализов.

Результаты анализов:

[ANY.RUN анализ и обзор >>](#)

[Гибридный анализ >>](#)

[VirusTotal анализ >>](#)

Другой анализ >>

Степень распространённости: низкая.

Подробные сведения собираются регулярно.

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

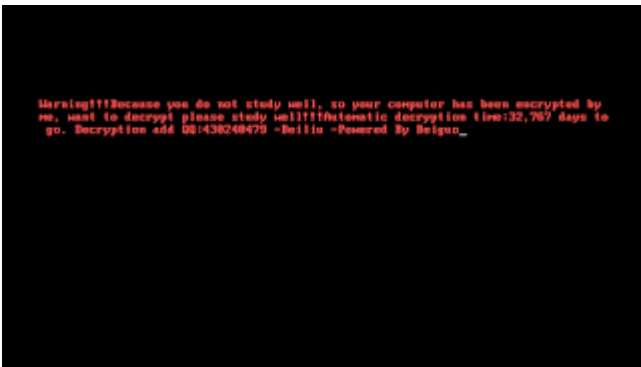
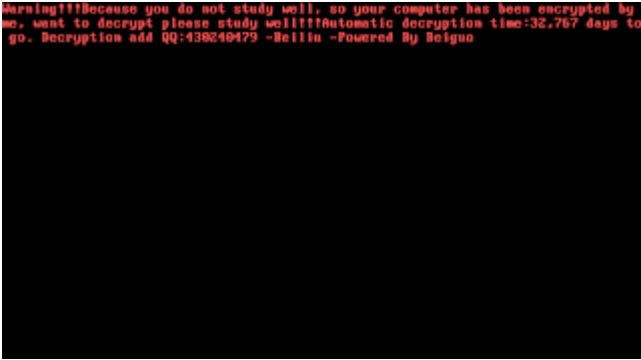
Вариант от 28 июня 2020:

Контакт в QQ: ID 3462958206 .

Результаты анализов: [VT](#) + [IA](#)

Вариант от 29 октября 2020:

Контакт в QQ: ID 430240479

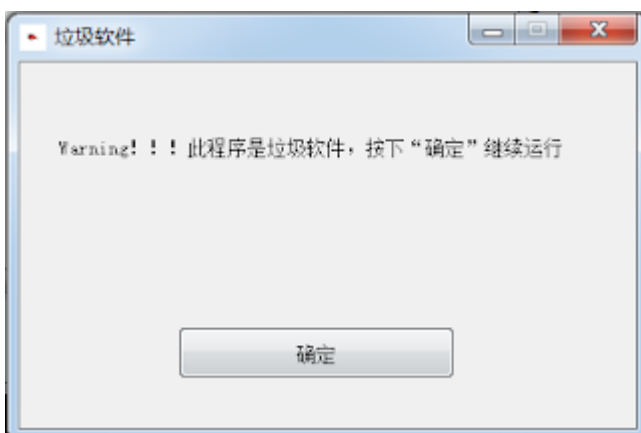


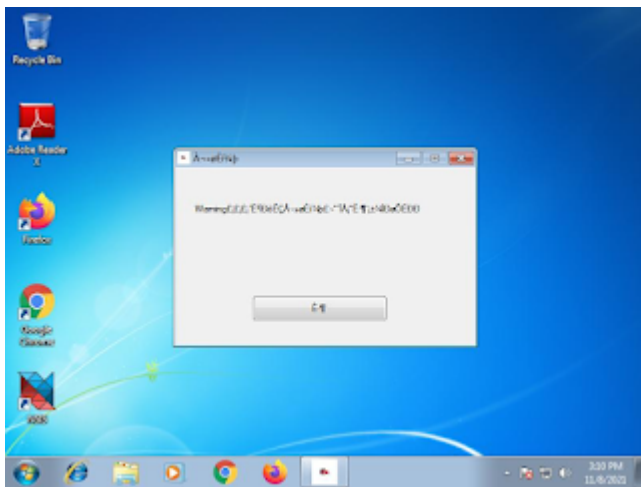
► Текст на экране:

Warning!!!Because you do not study well, so your computer has been encrypted by me, want to decrypt please study well!!!Automatic decryption time:32,767 days to go. Decryption add QQ:430240479 -Beiliu -Powered By Beiguo

Код для этого варианта: beiliu666NB

Также используется информационное диалоговое окно, которое можно закрыть.





Результаты анализов: [VT](#) + [IA](#)

► Обнаружения:

ALYac -> Trojan.Ransom.MBRlock

Avira (no cloud) -> TR/Ransom.MBRlock.kdilv

BitDefenderGeneric.Ransom.MBRLOCK.330538BF

DrWeb -> Trojan.MBRlock.301

ESET-NOD32 -> A Variant Of Win32/MBRlock.AQ

Kaspersky -> HEUR:Trojan-Ransom.Win32.Mbro.gen

Malwarebytes -> Ransom.MBRLOCK

Microsoft -> Ransom:Win32/Molock.A!bit

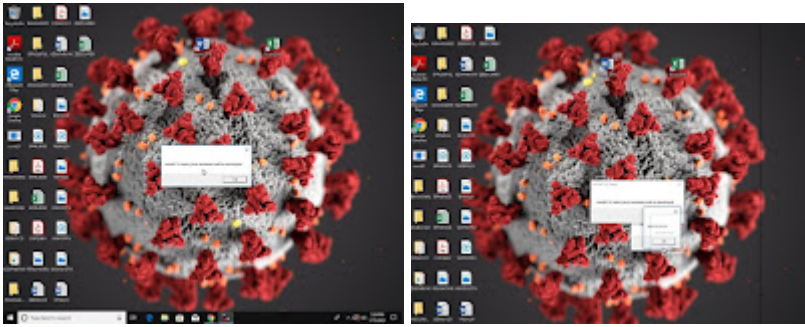
Rising -> Ransom.MBRlock!1.B6DC (CLASSIC)

Tencent -> Win32.Trojan.Mbro.Wtxk

TrendMicro -> Ransom.Win32.MBRLOCKER.SM

=== 2021 ===

Вариант от 5 января 2021:



Windows is killed by covid21
only thing you can do now is look
at blends surprise



Файлы: covid21.exe, covid.vbs, covid21.vbs, covid21.bat, screenscrew.exe, corona.vbs, covid.bmp,
PayloadMBR.exe, PayloadGDI.exe, CLWCP.exe

Результаты анализов: [VT](#) + [TG](#) + [IA](#)

► Обнаружения:

ALYac -> Trojan.Agent.KillMBR

Avira (no cloud) -> TR/KillMBR.NDS.1

BitDefender -> Dropped:Application.Joke.Blurscrn.A

DrWeb -> Trojan.KillMBR.24874

ESET-NOD32 -> A Variant Of Win32/KillMBR.NDS

Malwarebytes -> Ransom.Winlock

Microsoft -> Ransom:Win32/MBRLocker.DA!MTB

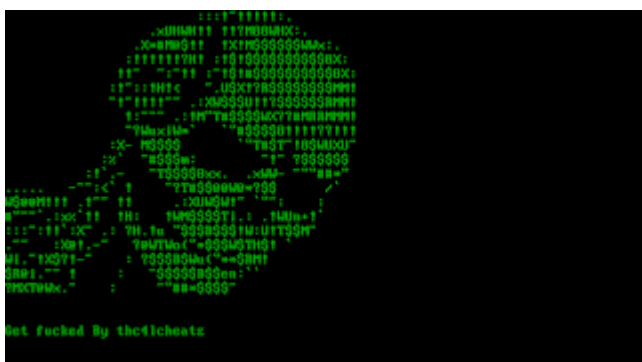
Rising -> Ransom.MBRLocker!8.F8C3 (CLOUD)

Tencent -> Win32.Trojan.Diskwriter.Dxni

TrendMicro -> Ransom.Win32.MBRLOCKER.THAABBA

Вариант от 6 января 2021:

Снимок экрана:



Файл: mbr lock.bin

Результаты анализов: [VT](#)

► Обнаружения:

ALYac -> Trojan.Ransom.MBRlock

DrWeb -> Trojan.Siggen9.27655

ESET-NOD32 -> A Variant Of Win32/KillMBR.NDS

Kaspersky -> Trojan.Win32.DiskWriter.ebe

Malwarebytes -> Trojan.MBRlock

Microsoft -> Trojan:Win32/Killmbr

Rising -> Trojan.KillMBR!1.C48A (CLASSIC)

TrendMicro -> Trojan.Win32.KILLMBR.AC

Вариант от 7 января 2021:

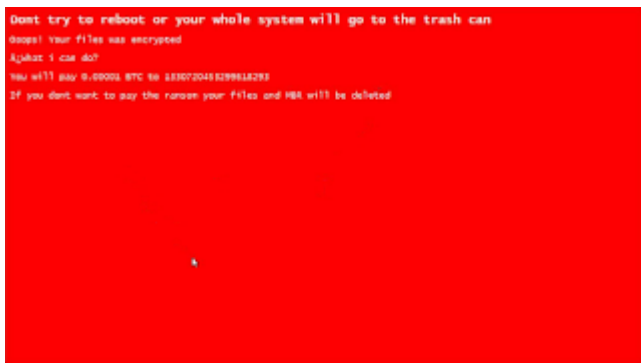
Результаты анализов: [VT](#) + [VT](#)

Снимки экрана:





Результаты анализов: [VT](#)



Вариант от 22 ноября 2021:

Файл: 1.exe

Результаты анализов: [VT](#)

► Обнаружения:

DrWeb -> Trojan.KillMBR.24875

BitDefender -> Trojan.GenericKD.38108433

ESET-NOD32 -> Win64/KillMBR.G

Kaspersky -> Trojan.Win64.Agentb.beg

Microsoft -> Trojan:Win32/Sabsik.FL.B!ml

Symantec -> Trojan.Gen.2

Tencent -> Win32.Trojan.Trojan.Ovoa

TrendMicro -> CallTROJ_GEN.R002H0CKP21

Вариант от 28 ноября 2021:

Файл: Cmd.Exe

Результаты анализов: [VT](#)

► Обнаружения:

DrWeb -> Trojan.KillMBR.24872

BitDefender -> Trojan.GenericKD.47511372

ESET-NOD32 -> A Variant Of Win32/KillMBR.NEJ

Kaspersky -> Trojan.Win32.DiskWriter.hdc

Microsoft -> Trojan:Win32/Sabsik.FL.B!ml

Symantec -> Trojan.Gen.MBT

TrendMicro -> TROJ_GEN.R002H0DKS21

Вариант от 18 декабря 2021:

Файл: DiskKiller-Clean.exe

Только показывает сообщение, не повреждая MBR.

Результаты анализов: [VT](#)

► Обнаружения:

DrWeb > Trojan.MBRlock.320

TrendMicro -> TROJ_GEN.R002H06LI21

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



Read to links:

[Tweet on Twitter](#) + [Tweet](#)

ID Ransomware

*

*



Added later:

[Write-up on BC](#) (added on February 10, 2018)

*



Thanks:

JAMESWT

ANY.RUN

Andrew Ivanov

Lawrence Abrams

© Amigo-A (Andrew Ivanov): All blog articles.

Source: <http://id-ransomware.blogspot.com.tr/2018/02/mbrlock-hax-ransomware.html>