VHD

Archived: 2026-04-05 17:15:59 UTC

VHD Ransomware

Aliases: VHDLocker

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей и организаций с помощью AES-128/256 (режим ECB) + RSA-2048, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: splwow32.exe. Написан на C++. Исследователи KasperskyLab считают, что VHD Ransomware принадлежит и управляется Lazarus Group.

Обнаружения:

DrWeb -> Trojan.MulDrop11.51552, Trojan.MulDrop16.42005
BitDefender -> Gen:Variant.Graftor.717353
Avira (no cloud) -> TR/Ransom.hrjej
ESET-NOD32 -> Win32/Filecoder.OBF
Kaspersky -> Trojan-Ransom.Win32.Agent.awny
Malwarebytes -> Ransom.Vhd
Microsoft -> Ransom:Win32/Cryptor!MSR
Rising -> Ransom.Cryptor!8.10A9 (CLOUD), Ransom.VHDLocker!1.C88A (CLOUD)
Symantec -> Downloader
TrendMicro -> Ransom_Cryptor.R011C0DCN20, Ransom.Win32.VHDLOCKER.B

© Генеалогия: VHD >> ChiChi и другие

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.vhd** **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 вторую половину марта 2020 г. Штамп даты: 19 марта 2020. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **HowToDecrypt.txt**

Содержание записки о выкупе:
All data on your pc were encrypted with strongest encryption method.
The only way to get your data back is to purchase unique key for you.
* You can get cheaper price if you contact us as soon as possible. *
After three days from now, it will be difficult to recover your data.
Good Luck.
contact address:
miclejaps@msgden.net
stevenjoker@msgden.net

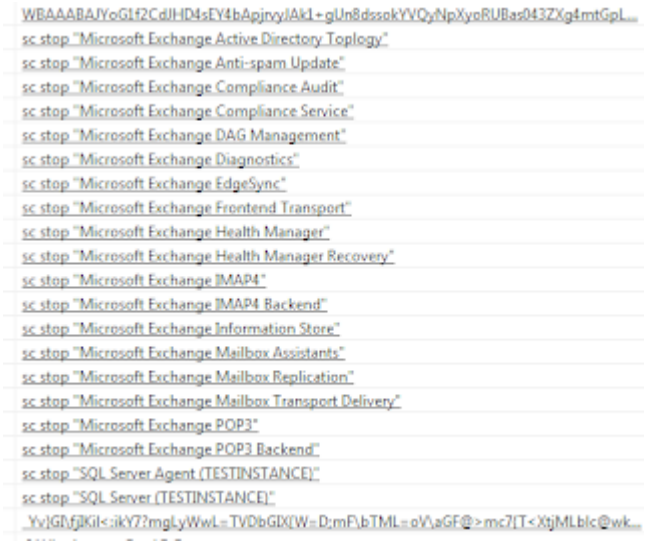
Перевод записки на русский язык:
Все данные на вашем пк зашифрованы надежным методом шифрования.
Единственный способ вернуть ваши данные - это приобрести уникальный ключ для вас.
* Вы можете получить меньшую цену, если напишите быстрее. *
Через три дня будет трудно восстановить ваши данные.
Удачи.
Контакт-адрес:
miclejaps@msgden.net
stevenjoker@msgden.net

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, 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**.

➤ Пытается остановить ряд служб согласно списку:
sc stop "Microsoft Exchange Active Directory Toplogy"
sc stop "Microsoft Exchange Anti-spam Update"
sc stop "Microsoft Exchange Compliance Audit"
sc stop "Microsoft Exchange Compliance Service"
sc stop "Microsoft Exchange DAG Management"
sc stop "Microsoft Exchange Diagnostics"
sc stop "Microsoft Exchange EdgeSync"
sc stop "Microsoft Exchange Frontend Transport"
sc stop "Microsoft Exchange Health Manager"
sc stop "Microsoft Exchange Health Manager Recovery"
sc stop "Microsoft Exchange IMAP4"
sc stop "Microsoft Exchange IMAP4 Backend"
sc stop "Microsoft Exchange Information Store"
sc stop "Microsoft Exchange Mailbox Assistants"
sc stop "Microsoft Exchange Mailbox Replication"
sc stop "Microsoft Exchange Mailbox Transport Delivery"
sc stop "Microsoft Exchange POP3"
sc stop "Microsoft Exchange POP3 Backend"
sc stop "SQL Server Agent (TESTINSTANCE)"
sc stop "SQL Server (TESTINSTANCE)"



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:
HowToDecrypt.txt - название файла с требованием выкупа
splwow32.exe
<random>.exe - случайное название вредоносного файла

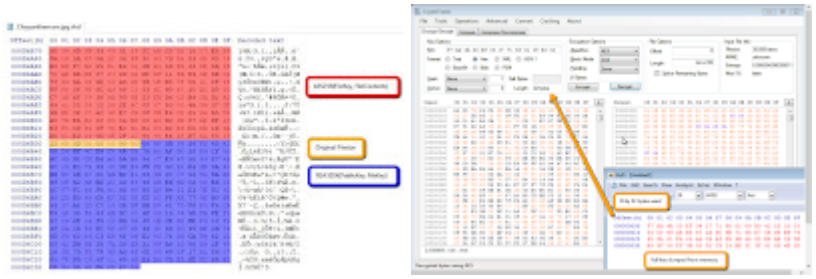
Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

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

Мьютексы:
AEEAEE SET

Сетевые подключения и связи:
Email: miclejaps@msgden.net, stevenjoker@msgden.net
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Скриншоты от исследователей:



CryptGenRandom генерирует 64-байтовый ключ, но AES использует только 32 байта.

```
for ( i = 0; i < 64; ++i )
  Key[i] = mt_rand(0, -1);
AES_KeyExpansion(_RoundKey, (unsigned __int8 *)Key);
```

```
unsigned int __stdcall mt_rand(int min, int max)
{
  int v2; // eax
  unsigned int v3; // ecx
  int i; // eax
  int N; // [esp+8h] [ebp-1398h]
  int v7[1248]; // [esp+Ch] [ebp-138Ch]
  int v8; // [esp+138Ch] [ebp-Ch]

  // Seed RNG
  v2 = std::tr1::_Random_device();              // s_rand (SystemFunction036 / CryptGenRandom)
  v7[0] = v2;
  v3 = v2;
  v8 = -1;
  for ( i = 1; i < 624; ++i )
  {
    v3 = i + 0x6C078965 * ((v3 >> 30) ^ v3);
    v7[i] = v3;
  }
  N = 624;
  return mt_rand1(min, max, (int)&N);
}
```

Результаты анализов:

Ⓗ **Hybrid analysis >>**

Σ VirusTotal analysis >>

🐞 **Intezer analysis >>**

⋟ **ANY.RUN analysis >>**

⧖ **VMRay analysis >>**

Ⓥ VirusBay samples >>

⩓ MalShare samples >>

👽 AlienVault analysis >>

🔃 CAPE Sandbox analysis >>

⟲ JOE Sandbox analysis >>

Степень распространённости: низкая.

Подробные сведения собираются регулярно. Присылайте образцы.

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

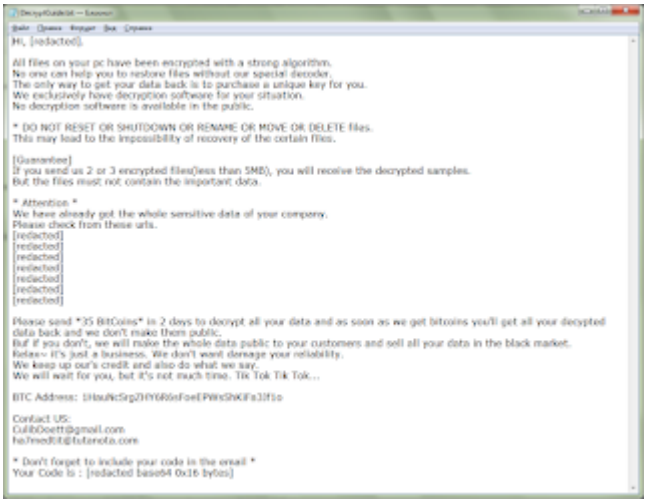
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Вариант от 5 июня 2020:

Расширение: **.0d0a**

Записка: DecryptGuide.txt

Email: CulibDoett@gmail.com, ha7medtit@tutanota.com



Обновление от 30 июля 2020:

Пост в Твиттере >>

Расширение: .vhd

Записка: HowToDecrypt.txt

Email: miclejaps@msgden.net, stevenjoker@msgden.net

Результаты анализов: **VT** + **IA** + **VMR** + **AR** + **JSB**

➤ Обнаружения:

DrWeb -> Trojan.MulDrop11.51552

BitDefender -> Trojan.GenericKD.43566381

ESET-NOD32 -> A Variant Of Win32/Filecoder.OBF

Kaspersky -> Trojan-Ransom.Win32.Agent.axwf

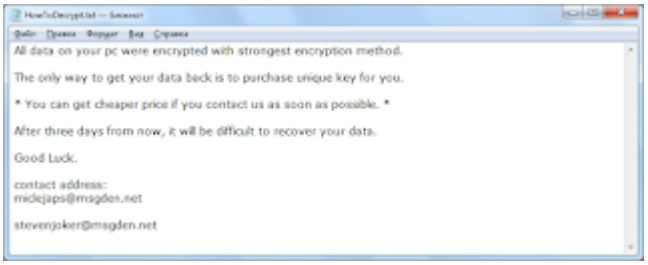
Malwarebytes -> Ransom.Vhd

Microsoft -> Ransom:Win32/Ymacco.AAA3

Rising -> Ransom.VHDLocker!1.C88A (CLOUD)

Tencent -> Win32.Trojan.Agent.Aojc

TrendMicro -> Ransom_Ymacco.R03BC0DH220



➤ Содержание записки:
All data on your pc were encrypted with strongest encryption method.
The only way to get your data back is to purchase unique key for you.
* You can get cheaper price if you contact us as soon as possible. *
After three days from now, it will be difficult to recover your data.
Good Luck.
contact address:
miclejaps@msgden.net
stevenjoker@msgden.net

Вариант от 7 апреля 2021:

Расширение: **.beaf**

Записка: DecryptGuide.txt
Email: ha7medtit@tutanota.com, araujosantos@protonmail.com

Результаты анализов: **VT** + **IA**

➤ Обнаружения:

DrWeb -> Trojan.MulDrop16.42005

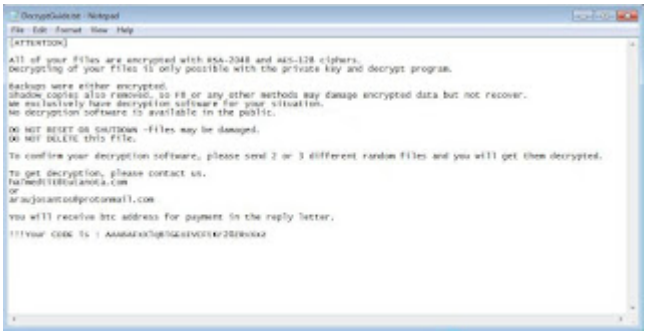
BitDefender -> Gen:Variant.Adware.ConvertAd.1427

ESET-NOD32 -> A Variant Of Win32/Filecoder.OBF

Microsoft -> Trojan:Win32/Genasom!MSR

Rising -> Ransom.Agent!1.C307 (CLOUD)

TrendMicro -> TROJ_GEN.R002C0DD721



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

Read to links:

Tweet on Twitter + Tweet + Tweet + myTweet

ID Ransomware (ID as VHD Ransomware)

Write-up, Topic of Support

*

Thanks:

Michael Gillespie, Jirehlov, GrujaRS

Andrew Ivanov (author)

***

to the victims who sent the samples
