

BlackMatter

Archived: 2026-04-05 22:30:50 UTC

BlackMatter Ransomware

(шифровальщик-вымогатель, RaaS) (первоисточник)

[Translation into English](#)



Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью Salsa20 + RSA-1024, а затем требует выкуп в BTC или XMR (Monero), чтобы вернуть файлы. Оригинальное название: BlackMatter Ransomware. Группа вымогателей и их представитель на хакерских форумах называют себя **BlackMatter**.

Обнаружения:

DrWeb -> Trojan.Encoder.34207

BitDefender -> Gen:Heur.Mint.Zard.25

ESET-NOD32 -> A Variant Of Generik.HLXFKFN

Kaspersky -> Trojan-Ransom.Win32.Encoder.njw

Malwarebytes -> MachineLearning/Anomalous.96%

Microsoft -> Ransom:Win32/Genasom

Rising -> Trojan.Generic@ML.98 (RDML:JZF*

Symantec -> ML.Attribute.HighConfidence, Ransom.Blackmatter, Ransom.Blackmatter!gm1

TrendMicro -> TROJ_GEN.R06CH09GQ21

© Генеалогия: ☼ [DarkSide](#), ☼ [REvil](#), ☼ [LockBit](#) >> **BlackMatter** > **LockBit 3.0 (LockBit Black)** с вариантами: **CriptomanGizmo** и другие.



Сайт "ID Ransomware" это идентифицирует как **BlackMatter**.

Информация для идентификации

Этот BlackMatter Ransomware был представлен на форумах кибер-андеграунда 21 июля 2021. Образец этого крипто-

вымогателя был найден в конце июля 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру. Известно о пострадавших крупных организациях в США, Великобритании, Канаде, Австралии, Индии, Бразилии, Чили и Таиланде, и это далеко не весь список стран.

К зашифрованным файлам добавляется случайное расширение: **.<random_id>**

Примеры таких расширений:

.51yupKSuX

.it2TiN2UtR

.gxtrGRlr6

Примечательно, что файлы могут шифроваться даже в Safe Mode (Безопасном режиме Windows).

Записка с требованием выкупа называется: **<random_id>.README.txt**



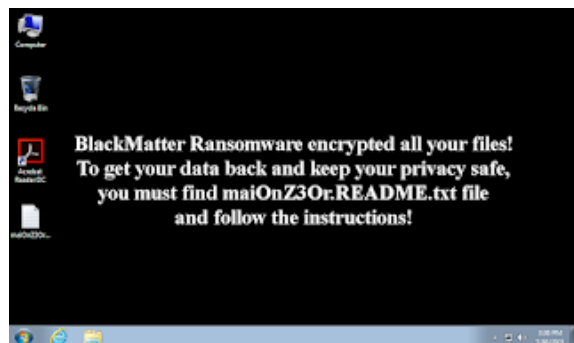
Примеры таких записок:

51yupKSuX.README.txt

gxtrGRlr6.README.txt

maiOnZ3Or.README.txt

Другим информатором жертвы является BMP-изображение с текстом, заменяющее обои Рабочего стола:



Это могут быть файлы:

51yupKSuX.bmp

gxtrGRlr6.bmp

maiOnZ3Or.bmp

Содержание записки о выкупе:

```

~+
      *   +
      '  BLACK   |
()  .-,='``'=,  - o -
      '=/_   \   |
*   | '=._   |
      \   `=./^,   '
      . '=._.= ' `=' *
+      Matter   +
      O   *   '   .

```

>>> What happens?

Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver.

We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.

>>> What guarantees?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.

If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals.

We always keep our promises.

>> Data leak includes

1. Full employees personal data
2. Network information
3. Schemes of buildings, active project information, architect details and contracts,
4. Finance info

>>> How to contact with us?

1. Download and install TOR Browser (<https://www.torproject.org/>).
2. Open [hxxx://supp24yy6a66hwszu2piygicgwzdtbwbftb76htfj7vni3getgqnxid.onion/7NT6LXKC1XQHW5039BLOV](https://supp24yy6a66hwszu2piygicgwzdtbwbftb76htfj7vni3getgqnxid.onion/7NT6LXKC1XQHW5039BLOV).

>>> Warning! Recovery recommendations.

We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.

Перевод записки на русский язык:

>>> Что происходит?

Ваша сеть зашифрована и в настоящее время не работает. Мы скачали с вашего файлового сервера 1 ТБ.

Нам нужны только деньги, после оплаты мы вам дадим дешифратор на всю сеть и вы восстановите все данные.

>>> Какие гарантии?

Мы не политически мотивированная группа, и нам не нужно ничего, кроме ваших денег.

Если вы заплатите, мы дадим вам программы для расшифровки и удалим ваши данные.

Если мы не дадим вам дешифраторы или не удалим ваши данные, нам никто не заплатит в будущем, это не наши цели.

Мы всегда выполняем свои обещания.

>> Утечка данных включает

1. Полные личные данные сотрудников
2. Сетевая информация
3. Схемы зданий, информация об активном проекте, детали архитекторов и контракты,
4. Финансовая информация

>>> Как с нами связаться?

1. Загрузите и установите браузер TOR (<https://www.torproject.org/>).

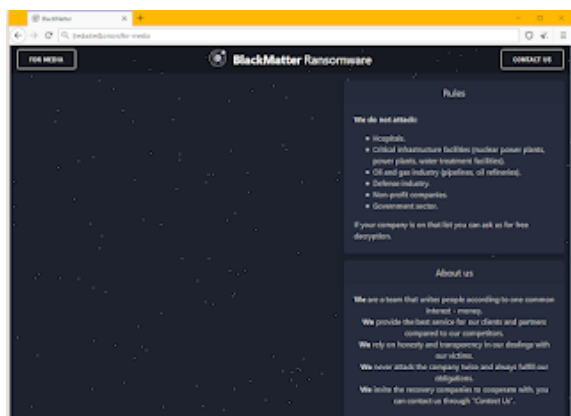
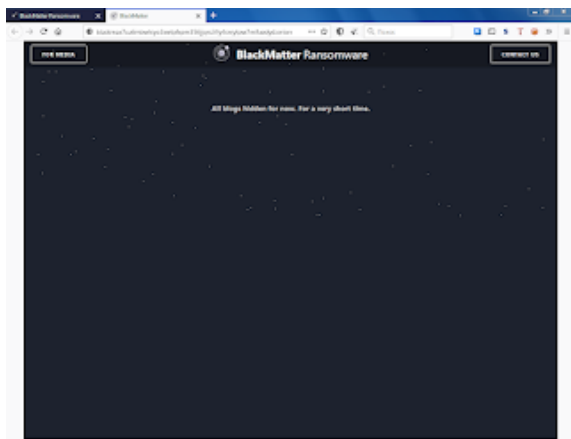
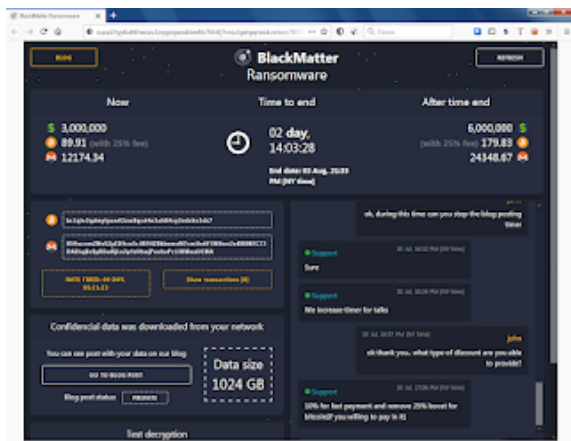
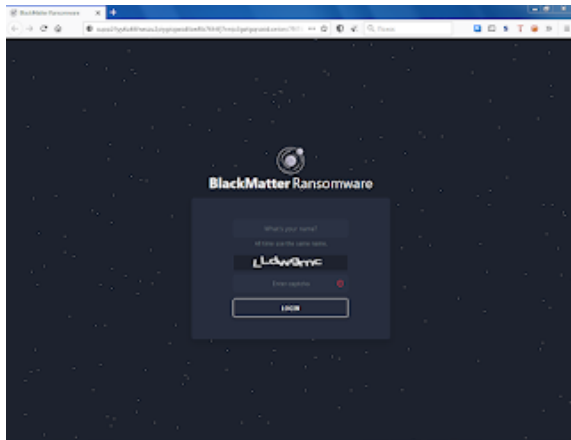
2. Откройте

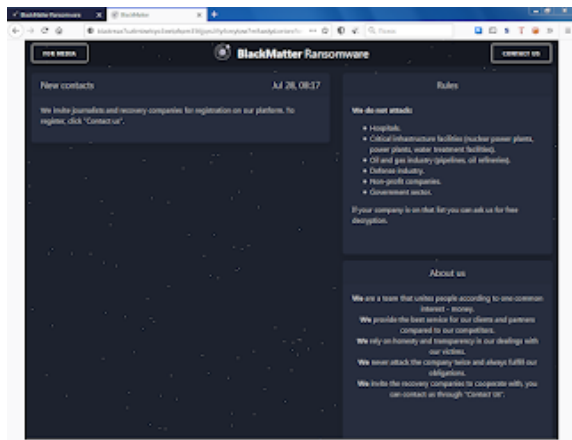
hxxx://supp24yy6a66hwszu2piyigcgwzdtbwftb76htfj7vnip3getgqnxid.onion/7NT6LXKC1XQHW5039BLOV.

>>> Внимание! Рекомендации по восстановлению.

Мы настоятельно рекомендуем вам не МОДИФИЦИРОВАТЬ и НЕ ИСПРАВЛЯТЬ ваши файлы, это может их повредить.

Полные скриншоты с сайта вымогателей





Изменения на 28 июля 2021

Содержание страницы "CONTACT US":

New contacts

We invite journalists and recovery companies for registration on our platform. To register, click "Contact us".

Rules

We do not attack:

Hospitals.

Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).

Oil and gas industry (pipelines, oil refineries).

Defense industry.

Non-profit companies.

Government sector.

If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.

We provide the best service for our clients and partners compared to our competitors.

We rely on honesty and transparency in our dealings with our victims.

We never attack the company twice and always fulfill our obligations.

We invite the recovery companies to cooperate with, you can contact us through "Contact Us".

Перевод страницы "CONTACT US":

НОВЫЕ КОНТАКТЫ

Правила

Мы не атакуем:

Больницы.

Объекты критической инфраструктуры (атомные и электростанции, водоочистные сооружения).

Нефтегазовая промышленность (трубопроводы, нефтеперерабатывающие заводы).

Оборонная промышленность.

Некоммерческие компании.

Государственный сектор.

Если ваша компания находится в этом списке, вы можете попросить нас о бесплатной расшифровке.

О нас

Мы - команда, объединяющая людей вокруг одного общего интереса - денег.

Мы предоставляем лучший сервис для наших клиентов и партнеров по сравнению с нашими конкурентами.

Мы полагаемся на честность и прозрачность в наших отношениях с нашими жертвами.

Мы никогда не атакуем компанию дважды и всегда выполняем взятые на себя обязательства.

Приглашаем к сотрудничеству компании, занимающиеся восстановлением, вы можете связаться с нами через «Контакты».



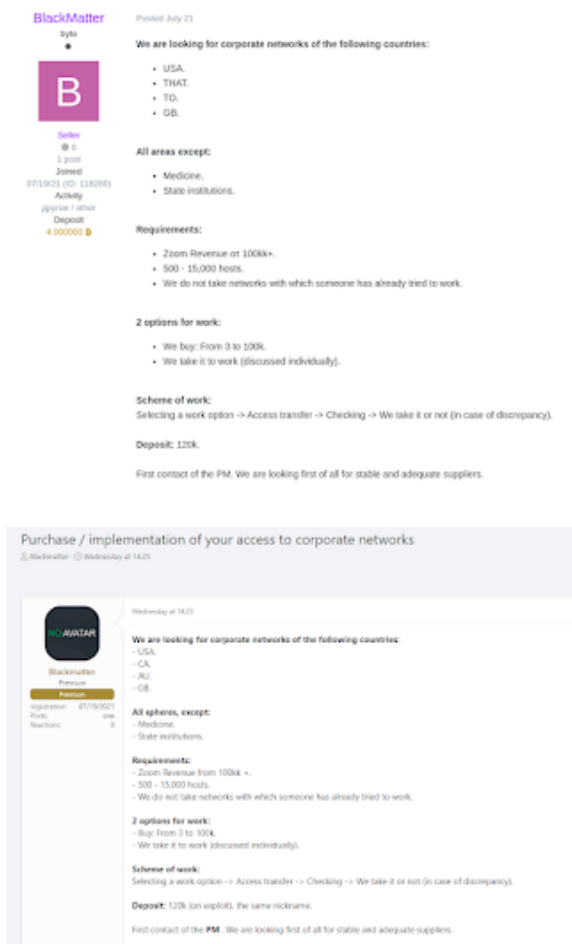
Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Могут быть различия с первым вариантом.

Технические детали + ИОС

На момент публикации этой статьи известно, что некто **BlackMatter** разместил объявления (фактически сделал рекламу) на форумах XSS и Exploit, несмотря на введенные на этих форумах в мае 2021 года запреты на рекламу и размещение программ-вымогателей. Поэтому объявления позиционируются как поиск "брокеров для начального доступа", то есть людей, которые имеют доступ к взломанным корпоративным сетям. Группа вымогателей BlackMatter нацелена на компании с доходом в 100 миллионов долларов и более.

Группировка BlackMatter называет брокерами тех, кто может предоставить им доступ к сетям крупных компаний с доходом \$100.000.000 в год или больше, с 500-15 000 хостами, базированием в США, Великобритании, Канаде, Австралии. Представитель BlackMatter заявляет, что подходящим по вышеназванным критериям брокерам они готовы заплатить до \$100.000 за эксклюзивный доступ к любой из подходящих сетей.

Представители BlackMatter внесли 4 BTC (около \$150,000) на эскроу-счёт на форуме Exploit, что подтверждает серьезность намерений злоумышленников, имеющих такую крупную сумму.



С момента открытия сайта утечек группа вымогателей с помощью своего BlackMatter Ransomware атаковала критически важные объекты инфраструктуры США, включая центры анализа крови и организации в продовольственном и сельскохозяйственном секторе.

Согласно заявлениям представителя поставщиков-вымогателей на хакерских форумах, группа BlackMatter не будет атаковать организации в нескольких отраслях, включая здравоохранение, критическую инфраструктуру, нефть и газ, оборону, некоммерческие организации и правительство. Это не является каким-то благородным жестом, это всего лишь реакция на ответные меры, введенные в этом году в США.

Поставщики-вымогатели утверждают, что их Ransomware реализован для разных версий ОС и архитектур и доступен в различных форматах, включая вариант Windows с поддержкой SafeMode (EXE/ReflectiveDLL/PowerShell) и вариант Linux с поддержкой NAS: Synology, OpenMediaVault, FreeNAS (TrueNAS). Они также утверждают, что Windows-вариант успешно протестирован на Windows Server 2003+ x86/x64 и Windows 7+ x64/x86, а Linux-вариант протестирован на ESXI 5+, Ubuntu, Debian и CentOS.

Вполне вероятно, что после успешного контакта партнёры вымогателей могут изменить первоначальный сценарий и начать распространять вредоносное ПО для шифрования файлов жертв путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, 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](#).

Список типов файлов, 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:

51urKSuX.README.txt - название файла с требованием выкупа;

51urKSuX.bmp - файл изображения с требованием выкупа;

<random>.exe - случайное название вредоносного файла.

History

Creation Time	2021-07-23 20:51:18
First Submission	2021-07-31 20:36:29
Last Submission	2021-07-31 20:36:29
Last Analysis	2021-08-01 09:31:13

Names

22d567c3af90bfa31f277ebabc2f6b4f625afbd543764377400e148bcc06d6eew
59bc530af8fe48f3f9f9792e48711a.virus

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2021-07-23 20:51:18
Entry Point	59606
Contained Sections	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	CHK2
.text	4036	55828	56320	6.79	2d2317b668b90eef7529f6ac33d3f33c	320624.63
.data	61440	976	1024	4.45	0f6e7428e9be6e2c4830c91f4e0ee458	43272.5
.rsrc	65536	5612	4096	7.59	58f4617131u5286a9774c101f6a50180	7385
.rsrc	73728	3495	3584	7.91	ec04060a92f1238a2f6be485act99a89	360.67
.ntsc	77824	2300	2560	6.43	5e842335de2021a2c268ac100ac513a5	18566.2

Расположения:

\Desktop\ ->

\User_folders\ ->

\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

Мьютексы:

См. ниже результаты анализов.

Сетевые подключения и связи:

Tor-URL: supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnxid.onion/*

Tor-URL: z4pgb74sb7gfbarspwojrl172niyx3455tgkgu6lyonq6zwswh2cpad.onion

Email: -

BTC: bc1qlv2qdmlyuw62zw8qcd4n3uh84cy2edckv3ds7

XMR:

85VxcvmZNVeZyED9cn5cJRFHZ8kbsmvN7cmUo6F3M6eo2xKB8KFC73DAEhqBc8yREwRjLo2pzfHtwjPoohvPcJJHMoaUCM

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

IOC: [VT](#), [HA](#), [IA](#), [TG](#), [AR](#), [VMR](#), [JSB](#)

MD5: 598c53bfef81e489375f09792e487f1a

SHA-1: 80a29bd2c349a8588edf42653ed739054f9a10f5

SHA-256: 22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6

Vhash: 064056651d7d7567z51z8nzafz

Imphash: c94b1566bf307396953c849ef18f9857

Степень распространённости: низкая.

Информация дополняется. Присылайте образцы.

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

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

1 августа 2021:

Специалисты Emsisoft получили образцы вредоносной программы и подтвердили, что BlackMatter является продолжением DarkSide. Самая первая версия BlackMatter оказалась почти идентичной последней версии DarkSide, но с незначительными улучшениями. За этой первой версией быстро последовало несколько новых итераций пейлоада BlackMatter, а затем его внутренний номер версии стал уже 2.0. [Ссылка на статью >>](#)

2 августа 2021:

Несколько цитат из этого интервью.

- Мы создали проект и вывели его на рынок в тот момент, когда ниша была свободна, а проект полностью соответствует требованиям рынка, поэтому его успех неизбежен.

- Атакованные нами компании уже общаются с нами. Пока переговоры ведутся успешно, мы не публикуем сообщения на главной странице блога.

- Пока мы делаем упор на долгосрочную работу. Мы также модерлируем цели и не разрешаем использовать наш проект для шифрования критически важной инфраструктуры, что привлечет к нам нежелательное внимание.

- Наш проект вообрал в себя сильные стороны каждой из партнерских программ: REvil, LockBit, DarkSide.

ALYac -> Trojan.Ransom.Filecoder

Avira (no cloud) -> HEUR/AGEN.1137758

BitDefender -> Trojan.GenericKD.46999490

DrWeb -> Trojan.Encoder.34334

ESET-NOD32 -> A Variant Of Win32/Filecoder.BlackMatter.C

Kaspersky -> Trojan-Ransom.Win32.BlackMatter.p

Malwarebytes -> Malware.AI.2096315471

Microsoft -> Ransom:Win32/BlackMatter.MAK!MTB

Rising -> Trojan.Generic@ML.97 (RDML:qyeJDApQr3Dfr2VT4pj7Hw)

Symantec -> Trojan.Gen.MBT

Tencent -> Malware.Win32.Gencirc.10cee34b

TrendMicro -> Ransom.Win32.BLACKMATTER.SMYXBHMT

Новость от 1 ноября 2021:

Сообщается о закрытие проекта BlackMatter Ransomware.

Source: <https://id-ransomware.blogspot.com/2021/07/blackmatter-ransomware.html>