Maze, ChaCha

Maze Ransomware

Aliases: Maze Locker, MazeLocker, ChaCha, ChaChaLocker

Maze Doxware

(шифровальщик-вымогатель, публикатор) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей и компаний с помощью RSA + ChaCha20, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. Хакеры-вымогатели: Twisted Spider Extortion Group. Среди вымогателей есть граждане Украины, по другим данным это международная хакерская группа.

Смотрите видеообзор >>

Вымогатели, распространяющие Maze, могут публиковать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов с помощью программных средств (doxware). Об этих акциях вымогателей сообщалось в СМИ.

Обнаружения:
DrWeb -> Trojan.Siggen8.29003, Trojan.Encoder.30067
Bitdefender -> Gen:Heur.Ransom.Imps.1, Trojan.GenericKD.32704232
Malwarebytes -> Ransom.Maze
Symantec -> Trojan.Gen.MBT
VBA32 -> BScope.Trojan.Wacatac

© Генеалогия: Maze > Sekhmet > Egregor

Оригинальный логотип Maze Ransomware

Этимология названия:
В ранних вариантах не было никакого названия, потому мы использовали характерное слово ChaCha для названия и статьи. Не было никакого изображения, заменяющее обои Рабочего стола, а в html-записке вместо названия было нечто, сообщающее о системной ошибке: ~~0010 SYSTEM FAILURE 0010.~~ Именно так, зачеркнуто. Название на изображении, заменяющем обои, появилось в конце мая 2019, в более новых вариантах.

К зашифрованным файлам добавляется расширение: **.<random4-7>**

Примеры других расширений:
.rC0syGH
.DL1fZE
.LKc07P
.FBrRDWC
.t6brFnQ
.0HOgD
.MJNW

При этом, на одном ПК могут добавляться разные расширения к разным файлам. Принцип такой зависимости пока неясен.

Кроме того, в конец зашифрованных файлов добавляется маркер файлов: **0x66116166**

Это видно на скриншотах ниже, где этот маркер присутствует в разных файлах из разных ПК. Возможно, что это изменится позже, но на момент написания статьи и публикации это факт.

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 первую половину мая 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Первые пострадавшие были из США, дале список стран расширился.

Целевые отрасли:

Академическая

Авиация

Энергия

Финансовые услуги

Правительство

Здравоохранение

Производство

Средства массовой информации

Розничная торговля

Телекоммуникации

Технологии

Автомобильная промышленность

и прочие.

Записка с требованием выкупа называется: **DECRYPT-FILES.html**

Содержание записки о выкупе:

0010 SYSTEM FAILURE 0010

****

Attention! Your documents, photos, databases, and other important files have been encrypted!

****

The only way to decrypt your files, is to buy the private key from us.

You can decrypt one of your files for free, as a proof that we have the method to decrypt the rest of your data.

In order to receive the private key contact us via email:

getmyfilesback@airmail.cc

Remember to hurry up, as your email address may not be avaliable for very long.

Buying the key immediatly will guarantee that 100% of your files will be restored.

Below you will see a big base64 blob, you will need to email us and copy this blob to us.

you can click on it, and it will be copied into the clipboard.

If you have troubles copying it, just send us the file you are currently reading, as an attachment.

Base64:

M1ihuItJFJtvKrKaMGxt1UtaJoSTHI5dLA***

Красным выделены слова с ошибками.

Перевод записки на русский язык:

0010 SYSTEM FAILURE 0010

****

Внимание! Ваши документы, фото, базы данных и другие важные файлы зашифрованы!

****

Единственный способ расшифровать ваши файлы - это купить у нас закрытый ключ.

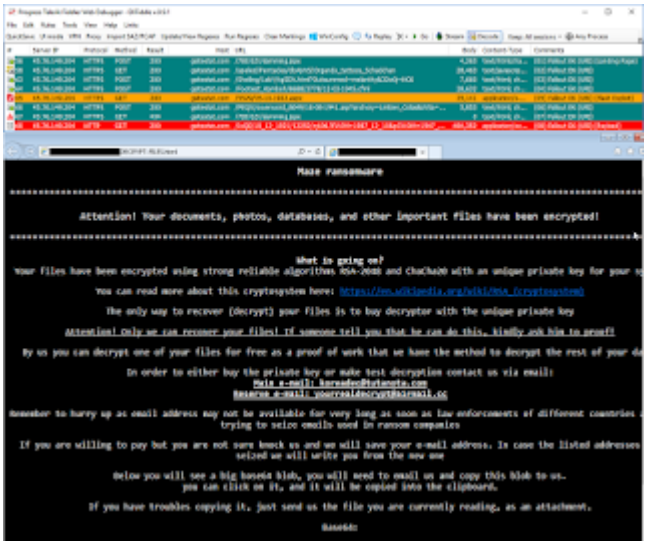
Вы можете бесплатно расшифровать один из ваших файлов в доказательство, что у нас есть метод для расшифровки остальных ваших данных.

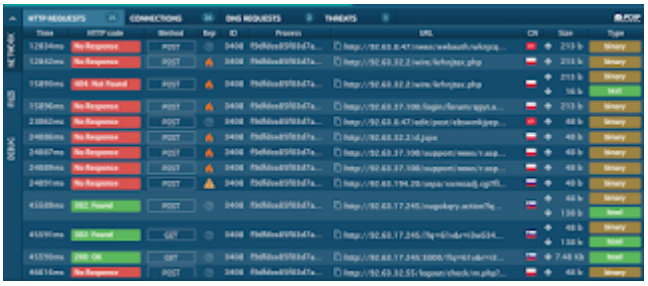
Чтобы получить закрытый ключ, контакт с нами по email:

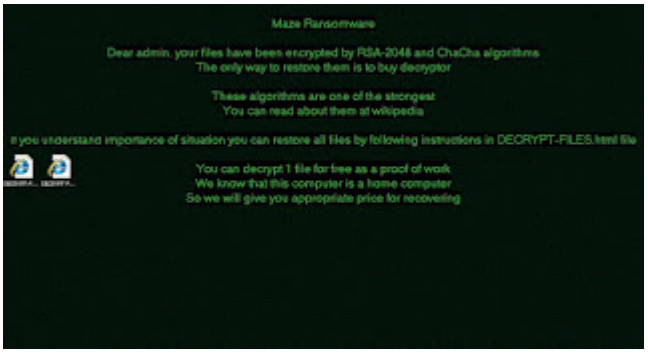
getmyfilesback@airmail.cc

Не забудьте поторопиться, т.к. ваш email-адрес может не будет доступен долго.
Покупка ключа немедленно гарантирует, что 100% ваших файлов будут восстановлены.
Ниже вы увидите большой блоб base64, вам нужно будет написать нам на email и скопировать этот блок в письмо.
Вы можете нажать на него, и он будет скопирована в буфер обмена.
Если у вас возникли проблемы с копированием, просто отправьте нам файл, который вы сейчас читаете, в виде вложения.
Base64:
M1ihuItJFJtvKrKaMGxt1UtaJoSTHI5dLA***

Другим информатором жертвы выступает изображение, заменяющее обои Рабочего стола.







Технические детали

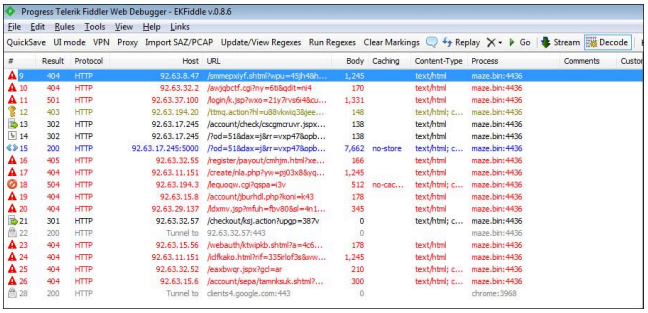
Распространяется с помощью набора эксплойтов **Fallout** через фальшивый сайт **Abra**, выдавая себя за приложение для обмена криптовалюты. Этот сайт создан для того, чтобы выдавать себя за рекламодателя и покупать трафик в рекламных сетях. Посетители этого сайта будут перенаправлены на специальную страницу, начиненную наборов эксплойтов, которые срабатывают при определенных условиях.

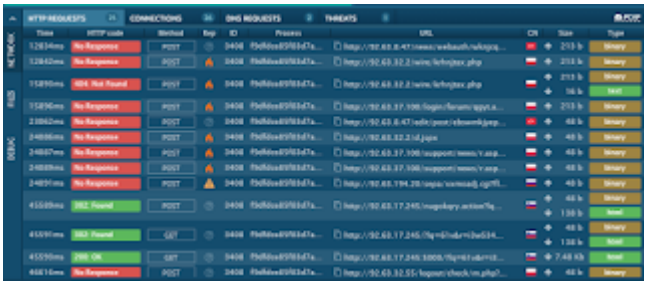
Может также распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, других эксплойтов, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей"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

➤ Этот Ransomware определяет тип ПК (домашний компьютер, рабочая станция, контроллер домен, сервером и пр.), а затем показывает соответствующую сумму выкупа, в тексте которого будет использована одна из следующих строк:
standalone server
server in corporate network
workstation in corporate network
home computer
primary domain controller
backup server
very valuable for you

➤ UAC не обходит. Требуется разрешение на запуск.
➤ Шифровальщик пытается подключиться к 15 сайтам (случайные URL-адреса) по IP-адресу, который начинается с 92. Сайты могут относиться к разным странам. См. список ниже.





➤ Другие деструктивные действия:
Создает файлы и изменяет сертификаты в каталоге Windows.
Записывает файлы в папку автозагрузки Word и меню Пуск.
Изменяет файлы в папке расширения Chrome и читает куки, видимо с целью кражи личных данных.

➤ Подключается к серверу без имени хоста.

➤ Группа, стоящая за распространением Maze и атаками, не гнушается доксингом, т.е. с целью давления на жертв угрожаем им обнародованием в Интернете похищенной информации, если не будет выплачен выкуп.

➤ Запрограммирован так, что проверят язык, используемый в компьютере и если этот язык находится в белом списке, то шифрование не производится.

Code	Language
0x419	Russian
0x422	Ukrainian
0x423	Belarusian
0x428	Tajik
0x42B	Armenian
0x42C	Azeri (Latin alphabet)
0x437	Georgian
0x43F	Kazakh
0x440	Kyrgyz
0x442	Turkmen
0x443	Uzbek (Latin alphabet)
0x444	Tatar
0x82C	Azeri (Cyrillic alphabet)
0x843	Uzbek (Cyrillic alphabet)
0x7C1A	Serbian
0x1C1A	Serbian (Bosnia and Herzegovina Cyrillic alphabet)
0x081A	Serbian (Latin alphabet)

В этом списке: русский, украинский, белорусский, таджикский, армянский, азербайджанский (латиница, кириллица), грузинский, казахский, киргизский, туркменский, узбекский (латиница, кириллица), татарский, сербский (латиница, кириллица) и боснийский.

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:
DECRYPT-FILES.html
foo.dat
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
%ProgramData%\foo.dat

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

Сетевые подключения и связи:
Email: getmyfilesback@airmail.cc
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
Ⓗ Hybrid analysis >>
Σ **VirusTotal analysis >>** **VT>>**
🐞 **Intezer analysis >>**
⧖ **VMRay analysis >>** **VMR>>**
Ⓥ VirusBay samples >>
⩓ MalShare samples >>
⪡ ANY.RUN analysis >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: **высокая**.
Подробные сведения собираются регулярно.

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

Maze Ransomware - май 2019 - ноябрь 2020

Sekhmet Ransomware - март 2020 - октябрь 2020

Egregor Ransomware - сентябрь 2020 - февраль 2021

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

Обновление от 14-15 мая 2019:

Пост в Твиттере >>

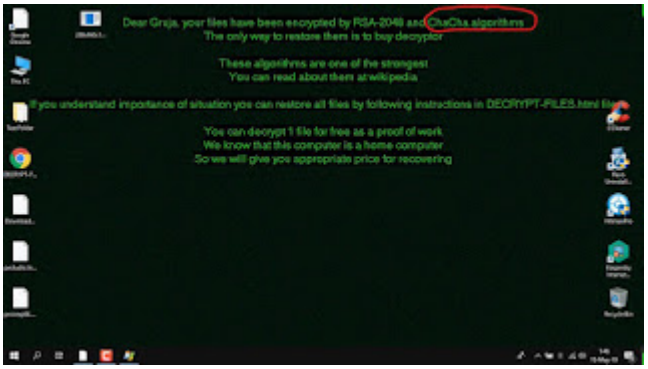
Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.html

Результаты анализов: **VT** + VMR

Также использует изображение, заменяющее обои Рабочего стола.

В текст записки добавляется имя пользователя.



Обновление от 29 мая 2019:

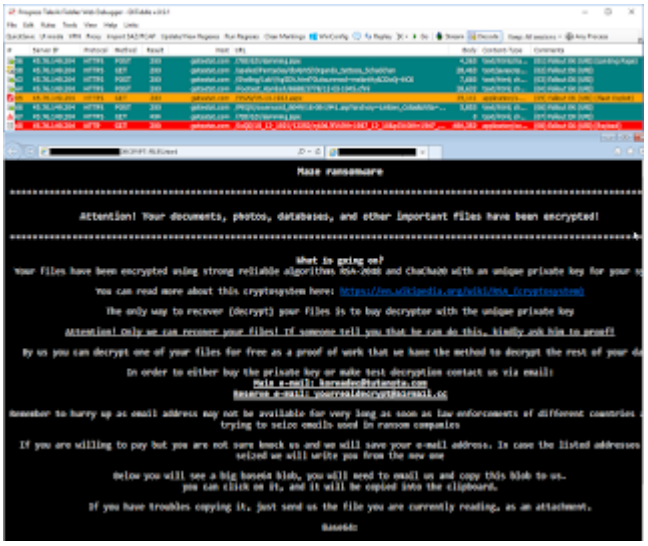
Пост в Твиттере >>

Самоназвание: Maze Ransomware

Расширение: .<random{4-7}>

Email: koreadec@tutanota.com

vourrealdecrypt@airmail.cc



Обновление от 31 мая 2019:

Самоназвание: Maze Ransomware

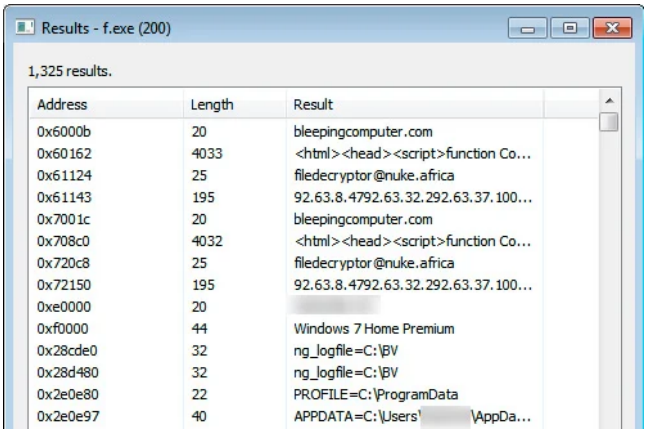
Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.html

Email: filedecryptor@nuke.africa

Результаты анализов: VT + VMR + IA + HA / VT + VMR

В статье Лоуренса Абрамса сообщается, что им обнаружен адрес bleepingcomputer.com в программной памяти Maze Ransomware. Точная задача неясна.



Обновление от 17 октября 2019:

[Пост в Твиттере >>]

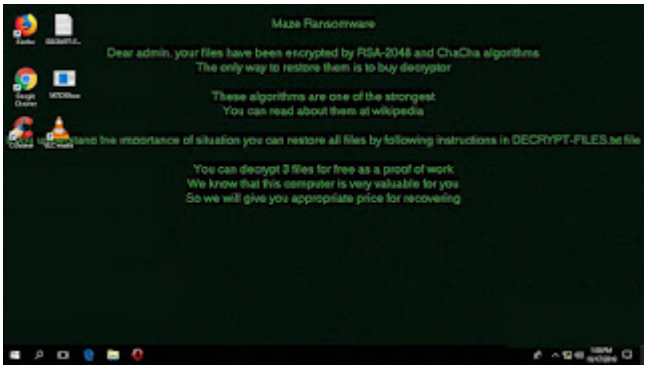
Самоназвание: Maze Ransomware

Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.html

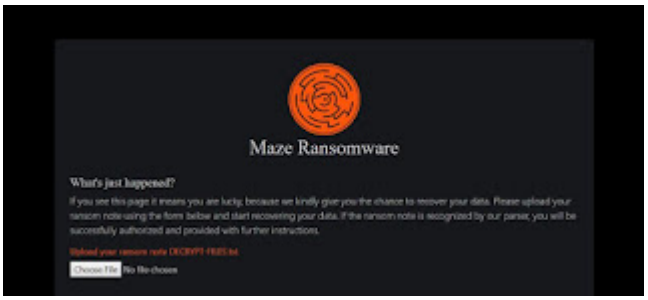
Результаты анализов: **VT** + **IA** + **AR**

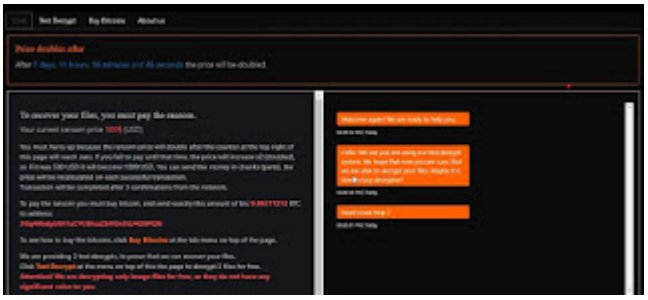
Скриншоты записки о выкупе и изображения, заменяющего обои Рабочего стола.



Видеообзор, сделанный с помощью сайта ANY.RUN

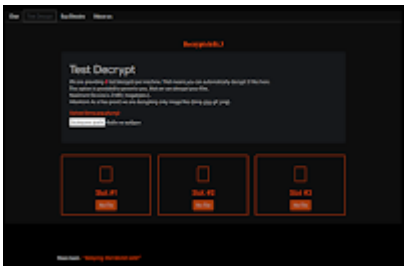
URL: hxxxs://mazedecrypt.top/***
Tor-URL: aoacugmutagkwctu.onion/***
Скриншоты с сайта вымогателей.

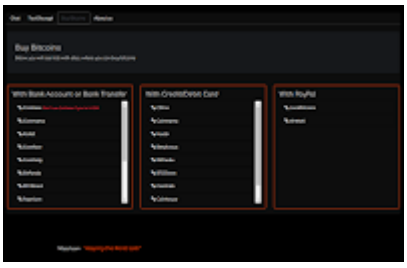


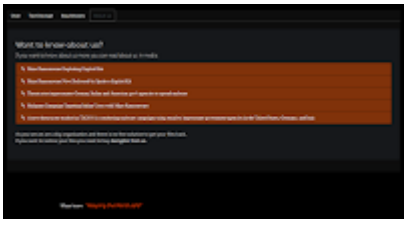


Обновление от 18 октября 2019:
Статья на сайте Bleeping Computer >>
В основном, представлен информация, опубликованная мною выше - 17 октября 2019. В дополнение к указанным мною данным можно добавить следующее.
Maze Ransomware теперь использует набор эксплойтов Spelevo в новой вредоносной кампании, использующей уязвимость Flash Player для атак на пользователей Сети. Ранее использовался набор эксплойтов Fallout. При перенаправлении на эксплойт Spelevo будет пытаться использовать уязвимость CVE-2018-15982. При этом уязвимыми будут пользователи Flash Player версий 31.0.0.153 / 31.0.0.108 и более ранних. После успешной эксплуатации уязвимости набор эксплойта автоматически загрузит и установит пейлоад с Maze Ransomware.
Обновление от 21 октября 2019:
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: .<random{4-7}>
Записка: DECRYPT-FILES.txt

URL: hxxxs://mazedecrypt.top/74980923c4ba3647
Tor-URL: hxxx://aoacugmutagkwctu.onion/74980923c4ba3647
Файл: ESET32.EXE
Результаты анализов: **VT** + **IA** + **AR** / **VT** + **AR**
Скриншоты с сайта mazedecrypt.top:





Содержание первой страницы:

Time is expired, fee was doubled.

To recover your files, you must pay the fee.

Your current fee 2400$ (USD)

You must hurry up because your 50% discount will expire after the counter at the top of this page will reach zero. If you fail to pay until that time, the fee will be increased x2 (doubled), so if it was 2400 USD it will become 4800 USD.

You can send the money in chunks (parts), the fee will be recalculated on each successful transaction.

Transaction will be completed after 3 confirmations from the network.

To pay the fee you must buy bitcoin, and send exactly this amount of btc 0.3221922 BTC to address:

3NQ1JyX5iphB9PhAyawMCkyS8iV1xzoTpT

To see how to buy the bitcoins, click Buy Bitcoins at the tab menu on top of the page.

We are providing 3 test decrypts, to prove that we can recover your files.

Click Test Decrypt at the menu on top of this the page to decrypt 3 files for free.

Attention! We are decrypting only image files for free, as they do not have any significant value to you.

Обновление от 29 октября 2019:

Пост в Твиттере >>

Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.txt

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

Обновление от 6 ноября 2019:

Пост в Твиттере >>

Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.txt

Обновление от 11-14 ноября 2019:

Пост в Твиттере >>

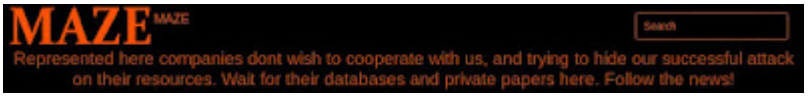
Пост в Твиттере >>

Расширение: .<random{4-7}>

Записка: DECRYPT-FILES.txt

Файл: eset.exe

Результаты анализов: **VT** + **HA** + **VMR** / **VT**



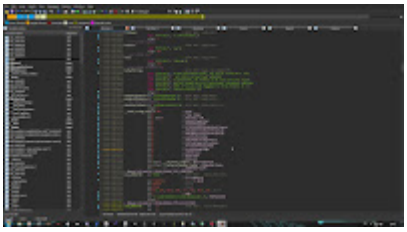
Обновление от 12 декабря 2019 года:

Статья от Emsisoft >>

Отчет и статистика о причиненном ущербе в США в 2019 году.

=== 2020 ===

Обновление от 29-30 января 2020:




В коде есть обращение к исследователям.
Kremez and Hasherezade. Two polish researchers. Why are still not married?
Cryptolnsane, be careful or we will lock your college and rename maze to Cryptolnsane ransomware
What if we pay some niggaman to throw Molotov to southwire office?

И еще одно разъяснение...

Теперь в записке сообщается о том, что нужно посмотреть в Гугле, что случилось с данными тех, кто не заплатил выкуп: компании Southwire, MDLab, город Pensacola.

Обновление от 5 марта 2020:
Пост в Твиттере >>


Maze Team official press release. June 22, 2020

Текст на английском:

Maze Team official press release. June 22, 2020
Maze Team is working hard on collecting and analyzing the information about our clients and their work. We also analyzing the post attack state of our clients How fast they were able to recover after the successful negotiations or without cooperation at all.
Today we would like to tell some words about the cost of non-cooperation and about our clients who were trying to recover all the information themselves. Looking ahead all those attempts were more close to suicide than to recovery.
So the company was attacked and the files were blocked and encrypted. What are the worst mistakes the company can made?

Maze Locker can't be decrypted without the help of Maze Team. A few companies we are not going to name were trying to decrypt the files with the help of side organizations. Those organizations are well known security companies. That happened at the end of 2019 and they are still waiting for a solution. As we know, compared to the first offer of Maze Team, those companies already paid two and a half times more money. One of those companies already spend four times more trying to decrypt the files themselves.
And we guarantee that it would take them years to wait until decryption.
But encrypting files is not the main risk. If the company have chosen to make a long pause in its operations this is the company's right But sometimes companies can't understand the risk of information leak, especially the private information We are specializing in client's private information, financial information, databases, credit card data. NDA documents and all the company's researches.
Usually that kind of information leaks will lead for multimillion losses, fines and lawsuits. And don't forget about the lost profit and falling of the stock price.
As we know from the reports of our clients the average recovery costs are about $60M We have never asked for amounts even close to those.
According to our statistics the loss from lawsuits and fines varies from $18M to $47M. As we know from one of our clients, in one week he loosed $12M while his files were in open access. For large companies the average lost if about $50M-60M after the publication of private data. A few very large companies have lost from $250M to $350M.
While hiring the negotiators from the side, especially the those who work on government, and listening to what they tell you, try to think are they really interested in solving your problems or they are just thinking about their own profit and ambitions of the government agency they belong to They can't minimize your loss or eliminate the data breach You'll pay from your own pocket.
But you will be able to find yourself in a statistics of companies who were proudly refuse to pay to minimize the loss of attack.
***

Перевод текста на русский:

Официальный пресс-релиз Maze Team. 22 июня 2020 г.

Команда Maze собирает и анализирует информацию о наших клиентах и их работе. Мы также анализируем состояние наших клиентов после атаки. Как быстро они смогли восстановиться после успешных переговоров или вообще без сотрудничества.
Сегодня мы хотели бы сказать несколько слов о цене отказа от сотрудничества и о наших клиентах, которые пытались восстановить всю информацию самостоятельно. Заглядывая вперед, все эти попытки были ближе к суициду, чем к восстановлению.
Таким образом, компания была атакована, а файлы были заблокированы и зашифрованы. Какие худшие ошибки может совершить компания?
Maze Locker не может быть расшифрован без помощи команды Maze. Несколько компаний, которые мы не хотим называть, пытались расшифровать файлы с помощью сторонних организаций. Эти организации являются хорошо известными security-компаниями. Это произошло в конце 2019 года, и они все еще ждут решения. Как известно, по сравнению с первым предложением Maze Team эти компании уже заплатили в два с половиной раза больше денег. Одна из этих компаний уже потратила в четыре раза больше, пытаясь расшифровать файлы самостоятельно.

И мы гарантируем, что им потребуются годы, чтобы дождаться расшифровки.
Но шифрование файлов не является основным риском. Если компания решила сделать долгую паузу в своих операциях, это право компании. Но иногда компании не могут понять риск утечки информации, особенно частной информации. Мы специализируемся на личной информации клиента, финансовой информации, базах данных, данных кредитной карты, документы NDA и все исследования компании. Обычно такие утечки информации приводят к многомиллионным убыткам, штрафам и судебным искам. И не забывайте о потерянной прибыли и падении курса акций.
Как мы знаем из отчетов наших клиентов, средние затраты на восстановление составляют около 60 миллионов долларов. Мы никогда не просили суммы, даже близкие к этим.
Согласно нашей статистике, убытки от судебных исков и штрафов варьируются от 18 до 47 миллионов долларов. Как мы знаем от одного из наших клиентов, за одну неделю он потерял 12 миллионов долларов, когда его файлы были в открытом доступе. Для крупных компаний средняя потеря составила около 50-60 млн долларов после публикации частных данных. Несколько очень крупных компаний потеряли от 250 до 350 миллионов долларов.
Нанимая переговорщиков со стороны, особенно тех, кто работает на правительство, и слушая то, что они вам говорят, старайтесь думать, действительно ли они заинтересованы в решении ваших проблем или просто думают о своей собственной прибыли и амбициях правительственного агентства. Они не могут минимизировать ваши потери или устранить утечку данных, которые вы заплатите из своего кармана.
Но вы сможете оказаться в статистике компаний, которые гордо отказывались платить, чтобы минимизировать потери от атак.
***

Обновление от 29 октября 2020:

Статья о закрытии вымогательского проекта "Maze Ransomware" и переход операторов-вымогателей на "Egregor Ransomware".

Вымогатели также подтверждили, что Maze, Sekhmet, Egregor являются их вымогательскими программами.

Более того, пострадавшие от Egregor после уплаты выкупа получают Sekhmet Decryptor.

Обновление от 1 ноября 2020:

Maze Team официально объявили о своем закрытии.


Maze Team official press release. November 1 2020

The Project is closed.

Maze Team Project is announcing it is officially closed.
All the links to our project, using of our brand, our work methods should be considered to be a scam.

We never had partners or official successors. Our specialists do not works with any other software. Nobody and never will be able to hold new partners at our news website. The Maze cartel was never exists and is not existing now. It can be found only inside the heads of the journalists who wrote about it.

Attention to everyone who wants for its private information to be deleted from our news website. You can contact to Maze support chat. Support will be continued for a month after the press-release.

There were a lot of rumors, lies and speculations around our project. So we decided to answer the questions "why" and "what for".

WHY? Our world is sinking in the recklessness and indifference, in laziness and stupidity. If you are risking the responsibility for other people money and personal data then try to keep it secure. Until you do that there will be more projects like Maze to remind you about secure data-storage.

How come that you don't understand that right now a hacker attack is enough for a large area or a country to lose the access to internet, water, gas and electricity. As an instance we had the access to state life support systems of New Yorks and to major internet providers. A good attack was able to cut the access to internet for 35 years. We didn't attack these objects but their security is still disgusting. Think about it. It's not the private case but the security of the whole country and its citizens. One day whose open doors will be pierced not by Maze but by some radical psychos whose goals will not just to show you the weakness of security but to make a major damage.

What for? Our world is turning into digital detention camp. Ten or fifteen years and nobody will be able to stay aside the system without the fear to lose its social status. Without that social status you won't be able to make purchases or get the social benefits. The first sign was the bitcoin. The digital currency existing only inside the digital world. After some time it will allow its owners to rule the world and to crush the economy of other countries as the gold and currency reserves are not converting into bitcoin. More and more people will work online to be paid with digital currencies. And all the job will be online.

Crypto-currencies are going higher and higher and after some time the price will reach a million dollars for a single coin. When all the coins will be dumped by its owners to buy real money. So all the bitcoins will be concentrated by a few people so they will be able to transform the world to a digital platform by ruining it.

With all your recklessness, weaknesses and stupidity you are pushing the the world into it. You are slowly turning into a controllable flock. You would not even notice when you will be tagged with chips or your DNA will be the only way to access the new digital world. As it will be the only place you can learn in, to get paid and consume.

All your technologies are a symbol of your helplessness. Once going to wheelchair a man will not be able to walk again. And once trusting your mind to a technology you won't be able to recover your consciousness. By delegation the part of your conscious activity to machines you won't be able to watch at the reality with the clear eye.

You are calling the ones who are killing your mind as your friends and support. And you also calling the ones who are showing you your weakness as the foes and molesters. The modern world is confusing the cause and the effect, the good and the evil.

Think about it. Try to prevent it. You think that the modern world is a hell. But it's just coming and you are doing much for it.

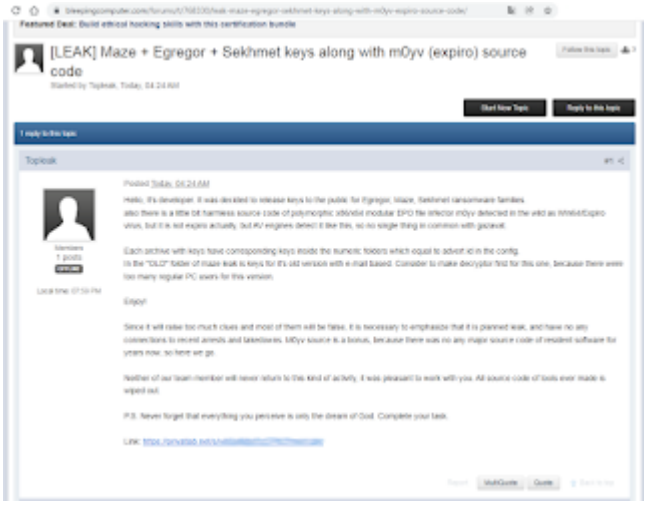
We will be back to you when the world will be transformed. We will return to show you again the errors and mistakes and to get you out of the Maze.

Я также объявляю о закрытии этой темы и статьи.

Новость от 9 февраля 2022

Представитель группы вымогателей выложил в общий доступ на форуме BleepingComputer ключи дешифрования для пострадавших от Maze, Sekhmet, Egregor Ransomware.

Ссылка на скриншоте скрыта, чтобы не дать возможность использовать вредоносные файлы инфектора m0yv, которые были в архиве.



Внимание!

Теперь есть дешифровщик >>

Вариант от 10 июня 2022:

Расширение: .<random>

Пример расширения: .wMbix3

DECRYPT-FILES.txt

Tor-URL: hxxx://aoacugmutagkwctu.onion/486b0bd5c056dd08

Сайт: hxxxs://mazedecrypt.top/486b0bd5c056dd08

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

Read to links:

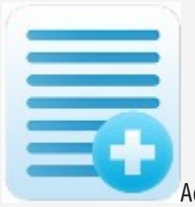
[Tweet on Twitter](#) + [Tweet](#) + [myTweet](#)

ID Ransomware (ID as ChaCha)

Write-up, [Topic of Support](#)

🎥 [Video review >>](#)

- Видеообзор от Cyber Security GrujaRS



Added later:

[Write-up by BleepingComputer](#) (on May 31. 2019)

*

*

Thanks:

Michael Gillespie, GrujaRS

Andrew Ivanov (author)

*

to the victims who sent the samples
