Moisha

id-ransomware.blogspot.com/2022/08/moisha-ransomware.html

Moisha Ransomware

PT_MOISHA Hacking Team

Moisha Doxware

(хакерская группа, шифровальщик-вымогатель, публикатор) (первоисточник)
Translation into English

Эта хакерская группа использует крипто-вымогатель, чтобы шифровать данные атакованных бизнес-пользователей, а затем сообщает, что сеть взломана, а данные украдены. Вымогатели требуют выкуп в $10000, чтобы не публиковать украденные файлы и получить дешифровщик для расшифровки файлов. Оригинальное название: Moisha, а название группы PT_MOISHA team. На файле написано: lsassd.exe.

Обнаружения:
DrWeb -> Trojan.Encoder.35760
BitDefender -> Trojan.GenericKD.61278257
ESET-NOD32 -> MSIL/Filecoder.Hamster.A
Kaspersky -> HEUR:Trojan-Ransom.MSIL.Crypmod.gen
Malwarebytes -> Ransom.Filecoder.MSIL
Microsoft -> Ransom:Win32/Moisha!MSR
Rising -> Ransom.Crypmod!8.DA9 (CLOUD)
Tencent -> Msil.Trojan.Crypmod.Bplw
TrendMicro -> Ransom.MSIL.MOISHA.THHBBBB

© Генеалогия: родство выясняется >> Moisha

IDR IDENTIFIED ✕

Сайт "ID Ransomware" **Moisha** пока не идентифицирует.
Информация для идентификации

Активность этих вымогателей была в середине августа 2022 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

К зашифрованным файлам никакое расширение не добавляется.

Записка с требованием выкупа называется: **!!!READ TO RECOVER YOUR DATA!!! PT_MOISHA.html**

Содержание записки о выкупе:

Hi it's me PT_MOISHA
Our team has penetrated your corporate network!
What have we done?
1.We stole documents compromising your company:
_Projects!
__Client bases!
___Postal correspondence!
____Personal data of employees and customers!

2.When we left, we encrypted your computers with all the documents and left you this note!
We are waiting for you within 72 hours for negotiations, after this time we will gradually begin to destroy YOUR Business!
What do we plan to do with your documents?
1.We will carefully analyze everything that we have stolen from you, we are already doing it!
2.After analyzing the stolen projects, documents, personal data, we will start selling them on the black market!
3.We will organize the leak of your corporate documents, those that we do not need but are very important to you!
4.After complete sorting and analysis of the data, we will start mailing to your customers, having previously prepared the sitesleaks with your corporate data!
5.We will report your company's hack in the news and newspapers, it will be the collapse of your business!
6.After some time, we will begin to harass and terrorize your customers!
after some time, your documents, and projects that are not needed by us, will be available for everyone to view here!
http://moishddxqnpdxpababec6exozpl2yr7idfhdldiz5525ao25bmasxhid.onion
Use TorBrowser
!!!HOW TO AVOID ALL OF THIS!!!
We have good news for you, everything that happened, happened, but we can return everything! If we agree with YOU$
Cancel all actions with the sale, leakage and destruction of your reputation and the company as a whole! If we agree with YOU$
Let's get down to business!! WHAT DO WE WANT? we want MONEY) in exchange for money you get:
1.Decryptor to decrypt your files.
2. We will not sell your designs and documents.
3.We will remove all your files from our servers, this will stop your documents and projects from being leaked.
4. We will not terrorize your customers.
5. We will not report to the news and newspapers that you are not reliable and cannot be trusted.
6.We will tell your administrators how we penetrated your network, this is important for you!
THE PRICE OF OUR SILENCE: $10,000 usd!
Are you satisfied with our offer? Do you want to lose your reputation? Do you value your employees and partners? we're sure you don't want the hype! write to us:
In the first message, tell the operator your MOISHAID: AF042w38-h547-u295-1318-a081de5*****
for quick connection use: moisha_pt@mailfence.com
To start negotiations and restore data, use the Tox messenger, you can download it here https://tox.chat/
launch the messenger and add our operator as a friend, in the first message tell the operator MOISHAID !!
operator contact:
693E9B36480678C055A135337A72913FA16F704919BCEBDFC647ACB0BCACF160AA408304642B
We are waiting for you within 72 hours for negotiations, after this time we will gradually begin to destroy YOUR Business!
do not try to recover files yourself, this will lead to complete data loss!

Перевод записки на русский язык:

Привет, это я PT_MOISHA
Наша команда проникла в вашу корпоративную сеть!
Что мы наделали?
1. Мы украли документы, компрометирующие вашу компанию:
_Проекты!
__Клиентские базы!
___Почтовая переписка!
____Персональные данные сотрудников и клиентов!
2. Когда мы ушли, мы зашифровали ваши компьютеры всеми документами и оставили вам эту записку!

Ждем вас в течение 72 часов для переговоров, по истечении этого времени мы постепенно начнем разрушать ВАШ бизнес!
Что мы планируем делать с вашими документами?
1. Мы тщательно проанализируем все, что у вас украли, мы это уже делаем!
2.После анализа украденных проектов, документов, личных данных мы начнем продавать их на черном рынке!
3. Организуем утечку ваших корпоративных документов, которые нам не нужны, но очень важны для вас!
4.После полной сортировки и анализа данных, мы приступим к рассылке вашим клиентам, предварительно подготовив сайты утечки с вашими корпоративными данными!
5. Мы сообщим о взломе вашей компании в новостях и газетах, это будет крахом вашего бизнеса!
6. Через какое-то время мы начнем травить и терроризировать ваших клиентов!
через какое-то время ваши документы, и не нужные нам проекты, будут доступны для просмотра всем желающим здесь!
http://moishddxqnpdxpababec6exozpl2yr7idfhdldiz5525ao25bmasxhid.onion
Используйте TorBrowser
!!!КАК ВСЕГО ЭТОГО ИЗБЕЖАТЬ!!!
У нас для вас хорошие новости, все что было, то было, но мы можем все вернуть! Если мы согласны с ВАМИ $
Отмените все действия с продажей, утечкой и уничтожением вашей репутации и компании в целом! Если мы согласны с ВАМИ $
Давайте приступим к делу!! ЧТО МЫ ХОТИМ? мы хотим ДЕНЬГИ) в обмен на деньги вы получаете:
1. Decryptor для расшифровки ваших файлов.
2. Мы не будем продавать ваши проекты и документы.
3. Мы удалим все ваши файлы с наших серверов, это предотвратит утечку ваших документов и проектов.
4. Мы не будем терроризировать ваших клиентов.
5. Мы не будем сообщать в новостях и газетах, что вы ненадежны и вам нельзя доверять.
6. Мы расскажем вашим администраторам, как мы проникли в вашу сеть, это важно для вас!
ЦЕНА НАШЕГО МОЛЧАНИЯ: 10 000 долларов США !
Вы довольны нашим предложением? Вы хотите потерять свою репутацию? Вы цените своих сотрудников и партнеров? мы уверены, что вы не хотите шумихи! напишите нам:
В первом сообщении сообщите оператору свой MOISHAID: AF042w38-h547-u295-1318-a081de52e321
для быстрого подключения используйте: moisha_pt@mailfence.com
Для начала переговоров и восстановления данных используйте мессенджер Tox, скачать его можно здесь https://tox.chat/
запустить мессенджер и добавить в друзья нашего оператора, в первом сообщении указать оператора MOISHAID!!
контакт оператора:
693E9B36480678C055A135337A72913FA16F704919BCEBDFC647ACB0BCACF160AA408304642B
Ждем вас в течение 72 часов на переговоры, после этого времени мы постепенно начнем разрушать ВАШ бизнес!
не пытайтесь восстанавливать файлы сами, это приведет к полной потере данных!

✋ **Внимание!** Новые элементы идентификации: расширения, email, записки о выкупе можно найти в конце статьи, в обновлениях. Они могут отличаться от первого варианта.

Технические детали + IOC

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.

✋ **Внимание!** 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:
!!!READ TO RECOVER YOUR DATA!!! PT_MOISHA.html - название файла с требованием выкупа;

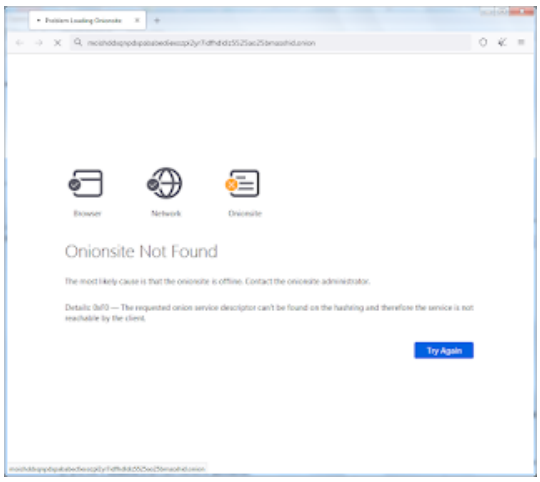
lsassd.exe - случайное название вредоносного файла;
<random>.exe - случайное название вредоносного файла.

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: hxxx://moishddxqnpdxpababec6exozpl2yr7idfhdldiz5525ao25bmasxhid.onion
Email: moisha_pt@mailfence.com
Tox
мессенджер: 693E9B36480678C055A135337A72913FA16F704919BCEBDFC647ACB0BCACF160AA408304642B
BTC: -
См. ниже в обновлениях другие адреса и контакты.



Сайт вымогателей для нас не открылся.

Результаты анализов:
IOC: **VT**, HA, IA, **TG**, AR, VMR, JSB

MD5: d197883d8745a61fe25aebea85622a65
SHA-1: 5d22d359e7b8dc70ccf5e369fb07f2e0960ef76f
SHA-256: b3ebc327773f5f846deeb1255475644a630c4d0d3b4eda3bbf995a36599c07cf
Vhash: 254036655511608c29130080
Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

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

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

Ещё не было обновлений этого варианта.

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

Read to links:

myMessage + Message + Message
Write-up, **Topic of Support**
***

Thanks:

Anneries, quietman7, MalwareHunterTeam
Andrew Ivanov (article author)
***
to the victims who sent the samples

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