Ako, MedusaReborn

id-ransomware.blogspot.com/2020/01/ako-ransomware.html

Ako Ransomware

Ako Doxware

Aliases: MedusaReborn

(шифровальщик-вымогатель, RaaS, публикатор) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные компьютеров в локальной сети, работающих под управлением Windows (в том числе Windows 10), с помощью AES, а затем требует выкуп в 0.5-1 BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Начиная с мая 2020 года вымогатели, стоящие за Ako Ransomware стали публиковать на специальном сайте украденные данные с целью усиления давления на жертву (отсюда дополнительные названия — публикатор и Doxware). Для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов. В некоторых случаях стали даже требовать дополнительной платы за то, чтобы удалить украденные данные.

Обнаружения:
DrWeb -> Trojan.MulDrop11.33124
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1
ESET-NOD32 -> Win32/Filecoder.MedusaLocker.D
Microsoft -> Ransom:Win32/MedusaLocker!MTB
Rising -> Ransom.AKO!1.C19E (CLOUD)

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: ✂️ MedusaLocker >> Ako, MedusaReborn ⇒ ThunderX > Ranzy Locker

Знак "⇒" здесь означает переход на другую разработку. См. "Генеалогия".

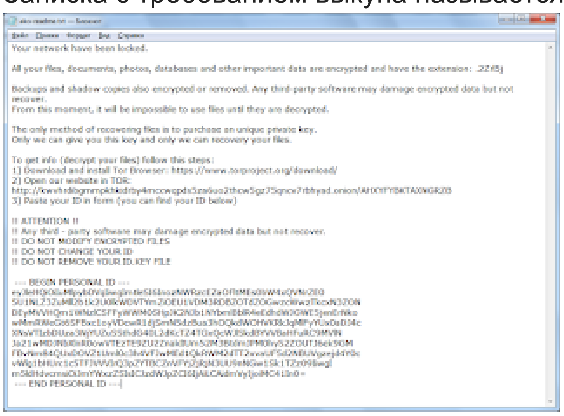
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.<random>** или **.<random{6}>**

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 начало января 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. На момент написания статьи распространялась версия 0.5.

Записка с требованием выкупа называется: **ako-readme.txt**


Your network have been locked.

All your files, documents, photos, databases and other important data are encrypted and have the extension: .2Zrl5j

Backups and shadow copies also encrypted or removed. Any third-party software may damage encrypted data but not recover.
From this moment, it will be impossible to use files until they are decrypted.

The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recovery your files.

To get info (decrypt your files) follow this steps:
1) Download and install Tor Browser: https://www.torproject.org/download/
2) Open our website in TOR:
[illegible]
3) Paste your ID in form (you can find your ID below)

!! ATTENTION !!
!! Any third - party software may damage encrypted data but not recover.
!! DO NOT MODIFY ENCRYPTED FILES
!! DO NOT CHANGE YOUR ID
!! DO NOT REMOVE YOUR ID.KEY FILE

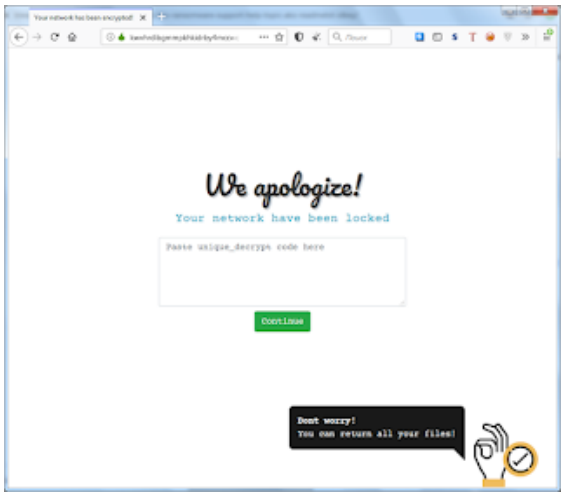
---- BEGIN PERSONAL ID ----
[illegible]
---- END PERSONAL ID ----

Содержание записки о выкупе:
Your network have been locked.
All your files, documents, photos, databases and other important data are encrypted and have the extension: .2Zrl5j
Backups and shadow copies also encrypted or removed. Any third-party software may damage encrypted data but not recover.
From this moment, it will be impossible to use files until they are decrypted.
The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recovery your files.
To get info (decrypt your files) follow this steps:
1) Download and install Tor Browser: https://www.torproject.org/download/
2) Open our website in TOR:

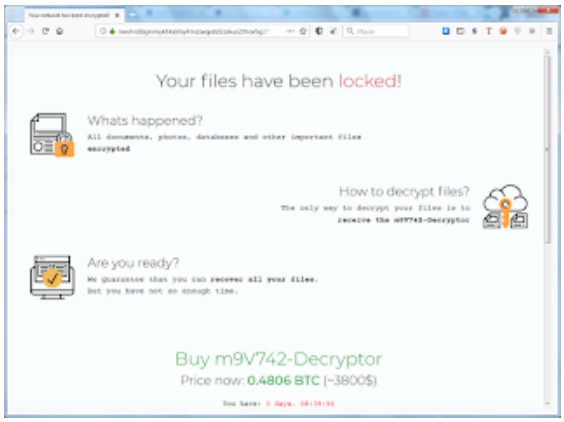
xxxx://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion/AHXYFYBKTAXNGRZB
3) Paste your ID in form (you can find your ID below)
!! ATTENTION !!
!! Any third - party software may damage encrypted data but not recover.
!! DO NOT MODIFY ENCRYPTED FILES
!! DO NOT CHANGE YOUR ID
!! DO NOT REMOVE YOUR ID.KEY FILE
--- BEGIN PERSONAL ID ---
eyJleHQiOiIuMlpybDVqIiwgImtleSI6InozNWRzcEZaOFltMEs0bW4xQVNrZE0
*** [всего 556 знаков]
--- END PERSONAL ID ---

Перевод записки на русский язык:
Ваша сеть заблокирована.
Все ваши файлы, документы, фотографии, базы данных и другие важные данные зашифрованы и имеют расширение: .2Zrl5j
Резервные копии и теневые копии также шифруются или удаляются. Любая сторонняя программа может повредить зашифрованные данные, но не восстановить.
С этого момента будет невозможно использовать файлы, пока они не будут расшифрованы.
Единственный способ восстановления файлов - это покупка уникального закрытого ключа.
Только мы можем дать вам этот ключ, и только мы можем восстановить ваши файлы.
Чтобы получить информацию (расшифровать ваши файлы), выполните следующие действия:
1) Загрузите и установите браузер Tor: https://www.torproject.org/download/
2) Откройте наш веб-сайт в TOR:
xxxx://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion/AHXYFYBKTAXNGRZB
3) Вставьте свой ID в форму (вы можете найти свой ID ниже)
!! ВНИМАНИЕ !!
!! Любая сторонняя программа может повредить зашифрованные данные, но не восстановить.
!! НЕ ИЗМЕНЯЙТЕ ЗАШИФРОВАННЫЕ ФАЙЛЫ
!! НЕ ИЗМЕНЯЙТЕ СВОЙ ID
!! НЕ УДАЛЯЙТЕ СВОЙ ID.KEY ФАЙЛ

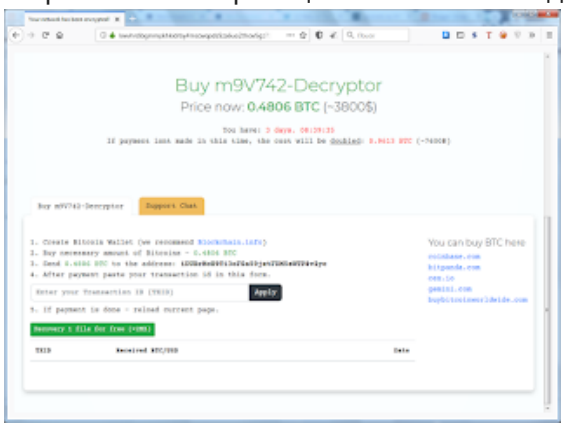
Запиской с требованием выкупа также выступает сайт вымогателей:



Начальная страница сайта, без ввода кода



Верхняя часть страницы сайта после ввода кода



Нижняя часть страницы сайта после ввода кода

Содержание страницы сайта:
Your files have been locked!
Whats happened?
All documents, photos, databases and other important files encrypted
How to decrypt files?
The only way to decrypt your files is to
receive the m9V742-Decryptor
Are you ready?
We guarantee that you can recover all your files.
But you have not so enough time.
Buy m9V742-Decryptor
Price now: 0.4806 BTC (~3800$)
You have: 3 days. 08:34:43
If payment isnt made in this time, the cost will be doubled: 0.9613 BTC (~7600$)
Buy m9V742-Decryptor
Support Chat
1. Create Bitcoin Wallet (we recommend Blockchain.info)
2. Buy necessary amount of Bitcoins - 0.4806 BTC
3. Send 0.4806 BTC to the address: 1DUBrMcH9T13oFSa59jxtFDM5eWTP8v2yc
4. After payment paste your transaction id in this form.
5. If payment is done - reload current page.

You can buy BTC here
coinbase.com

bitpanda.com
cex.io
gemini.com
buybitcoinworldwide.com

Перевод страницы сайта на русский язык:

Ваши файлы блокированы!
Что случилось?
Все документы, фотографии, базы данных и другие важные файлы зашифрованы
Как расшифровать файлы?
Единственный способ расшифровать ваши файлы - это получить m9V742-Decryptor
Вы готовы?
Мы гарантируем, что вы можете восстановить все ваши файлы.
Но у вас не так много времени.
Купить m9V742-Decryptor
Цена сейчас: 0.4806 BTC (~ 3800 $)
У вас есть: 3 дня. 8:34:43
Если оплата не будет произведена в это время, стоимость будет удвоена: 0,9613 BTC (~ 7600 $)
Купить m9V742-Decryptor
Чат поддержки
1. Создайте биткойн-кошелек (мы рекомендуем Blockchain.info)
2. Купите необходимое количество биткойнов - 0.4806 BTC
3. Отправьте 0,4806 BTC по адресу: 1DUBrMcH9T13oFSa59jxtFDM5eWTP8v2yc
4. После оплаты вставьте идентификатор вашей транзакции в эту форму.
5. Если оплата сделана - перезагрузите текущую страницу.

Вы можете купить BTC здесь
coinbase.com
bitpanda.com
cex.io
gemini.com
buybitcoinworldwide.com

Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов (Rig EK), 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**.

➤ Удаляет теневые копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки командами:
vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
wmic.exe SHADOWCOPY /nointeractive

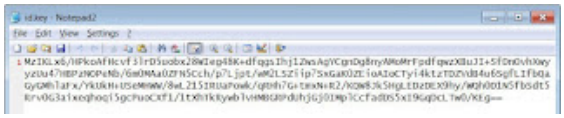
➤ Завершает работу ряда процессов и служб, относящихся к базам данных, бухгалтерии, корпоративных службам и пр., чтобы затем без препятствий шифровать их файлы:
MSSQL, MSSQLServer, SQL, MSExchange, QuickBooks, Firebird, WinDefend, IISADMIN и другие.

Список файловых расширений, подвергающихся шифрованию:
Почти все типы файлов, кроме пропускаемых.
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Пропускаемые типы файлов с расширениями:
.exe,. dll, .sys, .ini, .lnk, .key, .rdp

Пропускаемые папки с файлами:
AppData
Program Files
Program Files (x86)
AppData
boot
PerfLogs
ProgramData
Google
Intel
Microsoft
Application Data
Tor Browser
Windows
ako-readme.txt
id.key

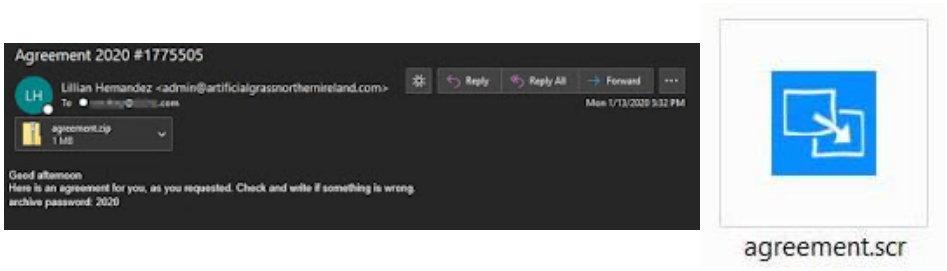
➤ Во время шифрования Ako использует функцию GetAdaptersInfo для получения списка сетевых адаптеров и связанных с ними IP-адресов. Затем выполняет проверку ping любых локальных сетей, используя функцию IcmpSendEcho, чтобы создать список отвечающих машин. Любые машины, которые ответят на запрос, будут проверены на наличие общих сетевых ресурсов для шифрования.



Когда вымогатель закончит работу, ключ шифрования, используемый для шифрования файлов

жертвы, тоже будет зашифрован и сохранен в файле с именем id.key на Рабочем столе жертвы.

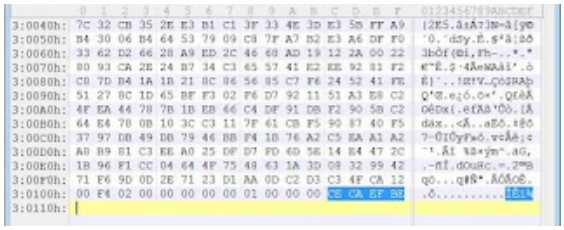
Файлы, связанные с этим Ransomware:
ako-readme.txt - название текстового файла
ak0.exe - исполняемый файл вымогателя;
ak0_new.exe - исполняемый файл вымогателя;
id.key
DllHost.exe
Agreement.zip (Agreement.scr) - email-вложение, которое устанавливает шифровальщика (пароль на архив - 2020).



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

Записи реестра, связанные с этим Ransomware:
HKEY_CURRENT_USER\Software\akocfg
См. ниже результаты анализов.

Файловый маркер:
CECAEFBE



Сетевые подключения и связи:
Tor-
URL: xxxx://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion/AHXYFYBKTAXNGRZB
Email: -
BTC: 1DUBrMcH9T13oFSa59jxtFDM5eWTP8v2yc
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

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 ===

Обновление от 15 января 2020:
Пост в Твиттере >>
Записка: ako-readme.txt. Содержание изменилось.
Версия обновлена с "0.5" до "1.0"
Слева v0.5, справа v1.0

➤ Содержание записки:
--- We apologize! ---
Your network have been locked.

| Whats happened?

All your files, documents, photos, databases and other important data are encrypted and have the ext
Backups and shadow copies also encrypted or removed. Any third-party software may damage encrypted

c***
From this moment, it will be impossible to use files until they are decrypted.
The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recovery your files.

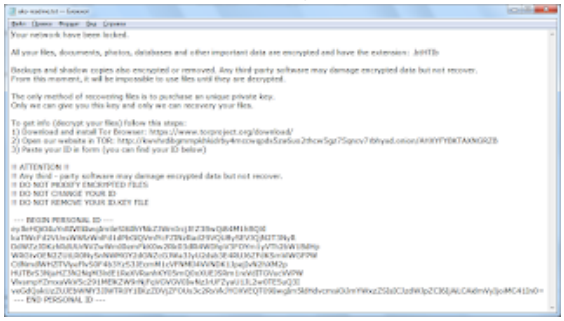
| Guarantees?

As you read above, files can be decrypted only using our private key and a special program.
The only guarantees we can give are decryption of your any file.
So you can decrypt any file from your system for free on our website.
We guarantee that you can recovery all your files. But you have not so enough time.

| How to recovery my files?

To get info (decrypt your files) you have 1 way:
1) [Recommended] via Tor Browser:
a) Download and install Tor Browser: https://www.torproject.org/download/
b) Open our website in TOR:
http://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion/
When you open our website, put the following key in the input form:
{PATTERN_ID}
!! ATTENTION !!
!! Any third - party software may damage encrypted data but not recover. !!
!! DO NOT MODIFY ENCRYPTED FILES !!
!! DO NOT CHANGE YOUR ID !!
!! DO NOT REMOVE YOUR ID.KEY FILE !!

Обновление от 11 января 2020:
Пост на форуме >>
Расширение: **.btHTIb**
Записка: ako-readme.txt
BTC: 19mXMJ3ZVY8eHjZpGcuq6M7hwGXDNnF64p

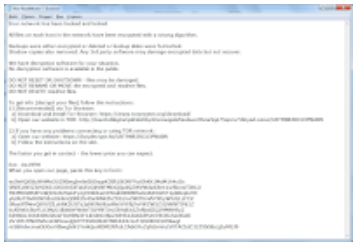


➤ Содержание txt-записки:
Your network have been locked.
All your files, documents, photos, databases and other important data are encrypted and have the extension: .btHTIb
Backups and shadow copies also encrypted or removed. Any third-party software may damage encrypted data but not recover.
From this moment, it will be impossible to use files until they are decrypted.
The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recovery your files.

To get info (decrypt your files) follow this steps:
1) Download and install Tor Browser: https://www.torproject.org/download/
2) Open our website in TOR:
http://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion/AHXYFYBKTAXNGRZB
3) Paste your ID in form (you can find your ID below)
!! ATTENTION !!
!! Any third - party software may damage encrypted data but not recover.
!! DO NOT MODIFY ENCRYPTED FILES
!! DO NOT CHANGE YOUR ID
!! DO NOT REMOVE YOUR ID.KEY FILE
--- BEGIN PERSONAL ID ---
eyJleHQiOiIuYnRlVEliIiwgImtleSI6IIh*** [всего 556 знаков]
--- END PERSONAL ID ---

➤ Содержание сайта вымогателей:

Your files have been locked!
Whats happened?
All documents, photos, databases and other important files encrypted
How to decrypt files?
The only way to decrypt your files is to
receive the btHTIb-Decryptor
Are you ready?
We guarantee that you can recover all your files.
But you have not so enough time.
Buy btHTIb-Decryptor
Price now: 0.3058 BTC (~3000$)
You have: 4 days. 01:11:52
If payment isnt made in this time, the cost will be doubled: 0.6117 BTC (~6000$)
Buy btHTIb-Decryptor Support Chat
1. Create Bitcoin Wallet (we recommend Blockchain.info)
2. Buy necessary amount of Bitcoins - 0.3058 BTC
3. Send 0.3058 BTC to the address: 19mXMJ3ZVY8eHjZpGcuq6M7hwGXDNnF64p
4. After payment paste your transaction id in this form.
[] [Apply]
5. If payment is done - reload current page.
[Download decrypted files]
***

Обновление от 16 марта 2020:
Пост в Твиттере >>
Расширение: **.Xs19FM**
Специальный файл: do_not_remove_ako.Xs19FM_id.key
Результаты анализов: **VT** + **AR**


Обновление от 12 мая 2020:
Ссылка на статью на сайте BleepingComputer >>
На специальном Leaks-сайте, созданном операторами Ako Ransomware, вымогатели сообщают, что некоторые компании должны платить выкуп как за дешифровщик. Так и за удаление украденных файлов. В качестве примера, Ако-вымогатели опубликовали данные одной из жертв и заявили, что они получили 350 000 долларов за дешифровщик, но всё равно опубликовали файлы после того, как не получили отдельную плату за удаление украденных файлов.

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

Read to links:

+ Tw + Tw + Tw + **myTweet**
ID Ransomware (ID as Ako / MedusaReborn)
Write-up, Write-up, **Topic of Support** + **Message**
*

Thanks:

S!Ri, Vitali Kremez, Raby, MHT, Michael Gillespie,
Andrew Ivanov (author)
Lawrence Abrams, Karsten Hahn
to the victims who sent the samples