# Meow

id-ransomware.blogspot.com/2022/09/meow-ransomware.html

## Meow Ransomware

## MeowCorp2022 Ransomware

## (ContiStolen Ransomware)

### (шифровальщик-вымогатель) (первоисточник)
### Translation into English

Этот крипто-вымогатель основан на коде, украденном у Conti-2 Ransomware, является его модифицированным вариантом. Он шифрует данные на взломанных серверах с помощью алгоритма ChaCha20, а затем требует связаться с вымогателями по email или в Telegram, чтобы узнать как заплатить выкуп и вернуть файлы. Оригинальное название: в заголовке записки есть фраза " MEOW! MEOW! MEOW!", а в логинах повторяется "meowcorp2022".

---

**Обнаружения:**
**DrWeb** -> Trojan.Encoder.35892
**BitDefender** -> Gen:Variant.Lazy.228618
**ESET-NOD32** -> A Variant Of Win32/Filecoder.Conti.R
**Kaspersky** -> HEUR:Trojan-Ransom.Win32.Conti.gen
**Malwarebytes** -> Ransom.Conti.Generic
**Microsoft** -> Ransom:Win32/Conti.IPA!MTB
**Rising** -> Ransom.Conti!1.DE02 (CLASSIC)
**Tencent** -> Win32.Trojan.Filecoder.Etgl

**TrendMicro** -> Ransom.Win32.CONTI.SMTH.hp
---

**© Генеалогия: CONTI-2 (stolen code) >> Meow**

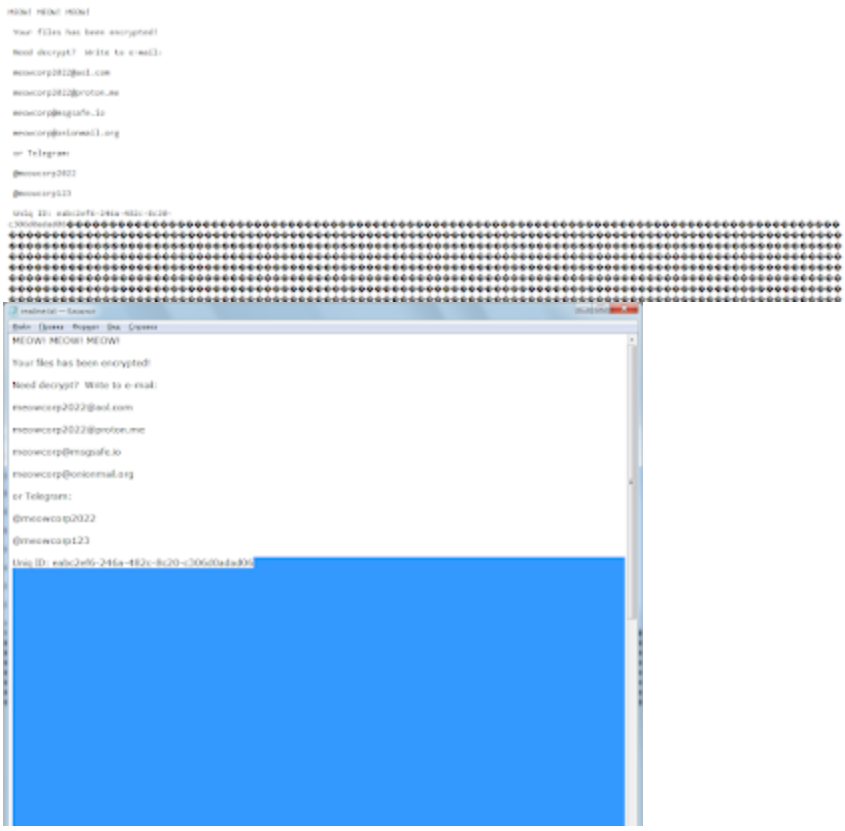
IDR IDENTIFIED

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

Активность этого крипто-вымогателя была в конце августа - в первой половине сентября 2022 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

К зашифрованным файлам добавляется расширение: **.MEOW**

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




На скриншотах записки, открытой в браузере и в обычном Блокноте, видно, что после

ID тянется еще шлейф пропусков или невидимых символов. Если будет повторяться в последующих вариантах, то это можно считать характерным признаком.

**Содержание записки о выкупе:**
MEOW! MEOW! MEOW!
Your files has been encrypted!
Need decrypt?  Write to e-mail:
meowcorp2022@aol.com
meowcorp2022@proton.me
meowcorp@msgsafe.io
meowcorp@onionmail.org
or Telegram:
@meowcorp2022
@meowcorp123
Uniq ID: eabc2ef6-246a-482c-8c20-c306d0ada***

**Перевод записки на русский язык:**
МЯУ! МЯУ! МЯУ!
Ваши файлы были зашифрованы!
Нужна расшифровка? Пишите на почту:
meowcorp2022@aol.com
meowcorp2022@proton.me
meowcorp@msgsafe.io
meowcorp@onionmail.org
или Telegram:
@meowcorp2022
@meowcorp123
Uniq ID: eabc2ef6-246a-482c-8c20-c306d0ada***

✋ **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.

**Список пропускаемых типов файлов:**

.exe и текстовые файлы записок.

**Файлы, связанные с этим Ransomware:**
readme.txt - название файла с требованием выкупа;
<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:**
Email: meowcorp2022@aol.com, meowcorp2022@proton.me, meowcorp@msgsafe.io, meowcorp@onionmail.org
Telegram: @meowcorp2022, @meowcorp123
BTC: -

См. ниже в обновлениях другие адреса и контакты.

**Результаты анализов:**

MD5: 033acf3b0f699a39becdc71d3e2dddcc
SHA-1: 5949c404aee552fc8ce29e3bf77bd08e54d37c59
SHA-256: 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853
Vhash: 025056655d15556az4oz15z27z
Imphash: 393974af133d6ece27fff97c28840d99

Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

---

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

---

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

**Вариант от 11-12 сентября 2022:**
Расширение: .MEOW
Записка: readme.txt
Email: meowcorp2022@aol.com
meowcorp2022@proton.me
meowcorp@msgsafe.io
meowcorp@onionmail.org

Telegram: @meowcorp321

@meowcorp123
@meowcorp2022

---

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


**Read to links:**

Message + Message + Message
Write-up, **Topic of Support**, **Topic of Support-2**
***


**Thanks**:

quietman7, Sandor, al1963
Andrew Ivanov (article author)
***
to the victims who sent the samples