0XXX

id-ransomware.blogspot.com/2021/06/0xxx-ransomware.html

0XXX Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные NAS-устройств WD (сетевых хранилищ Western Digital My Book) с помощью AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: 0XXX Virus. На файле написано: нет данных. Использует известные или новые уязвимости NAS-устройств.

Обнаружения:

DrWeb ->
ALYac ->
Avira (no cloud) ->
BitDefender ->
ESET-NOD32 ->
Kaspersky ->
Malwarebytes ->
Microsoft ->
Rising ->
Symantec ->
Tencent ->
TrendMicro ->

© Генеалогия: ✂ Kupidon + предыдущие для NAS-устройств >> 0XXX

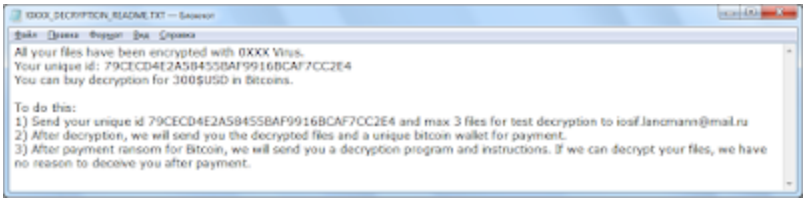
IDR IDENTIFIED ✓

Сайт "ID Ransomware" это идентифицирует как **0XXX**.
Информация для идентификации

Активность этого крипто-вымогателя была в середине июня 2021 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

К зашифрованным файлам добавляется расширение: **.0xxx**

Записка с требованием выкупа называется: **!0XXX_DECRYPTION_README.TXT**



Содержание записки о выкупе:
All your files have been encrypted with 0XXX Virus.
Your unique id: 79CECD4E2A58455BAF9916BCAF7CC2E4
You can buy decryption for 300$USD in Bitcoins.
To do this:
1) Send your unique id 79CECD4E2A58455BAF9916BCAF7CC2E4 and max 3 files for test decryption to iosif.lancmann@mail.ru
2) After decryption, we will send you the decrypted files and a unique bitcoin wallet for payment.
3) After payment ransom for Bitcoin, we will send you a decryption program and instructions. If we can decrypt your files, we have no reason to deceive you after payment.

Перевод записки на русский язык:
Все ваши файлы зашифровал 0XXX вирус.
Ваш уникальный идентификатор: 79CECD4E2A58455BAF9916BCAF7CC2E4
Вы можете купить расшифровку за 300 долларов в биткойнах.
Для этого:
1) Отправьте свой уникальный id 79CECD4E2A58455BAF9916BCAF7CC2E4 и максимум 3 файла для тест-расшифровки на iosif.lancmann@mail.ru
2) После расшифровки мы отправим вам расшифрованные файлы и уникальный биткойн-кошелек для оплаты.

3) После оплаты выкупа за биткойны мы вышлем вам программу расшифровки и инструкции. Если мы сможем расшифровать ваши файлы, у нас не будет причин обманывать вас после оплаты.

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

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.

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:
!0XXX_DECRYPTION_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: iosif.lancmann@mail.ru
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:

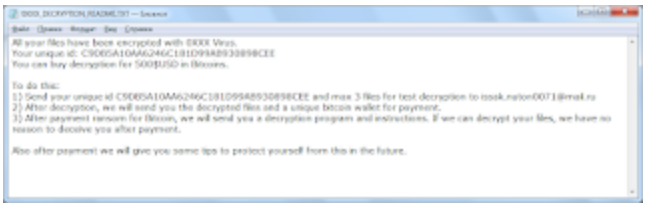
IOC: VT, HA, IA, TG, AR, VMR, JSB
MD5: -

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Сообщение от 24 июня 2021:
Статья на сайте BleepingComputer >>
Сообщается, что по всему миру NAS-устройства WD My Book Live получили удаленную команду на сброс настроек на заводские, при этом исчезли все разделы с находящимися на них файлами.
В отличие от устройств QNAP, которые обычно подключены к Интернету и подвержены атакам, таким как программы-вымогатели QNAPCrypt, QLocker, устройства Western Digital My Book хранятся за брандмауэром и обмениваются данными через облачные серверы My Book Live для обеспечения удаленного доступа.
Если у вас есть NAS-устройство Western Digital My Book, настоятельно рекомендуется отключить его от сети, пока инциденты не будут изучены.
Вариант от 28 августа 2021:
Расширение: .0xxx
Записка: !0XXX_DECRYPTION_README.TXT
Email: issak.nuton0071@mail.ru



Вариант от 14 нобря 2021:

Сообщение >>

Расширение: .0xxx

Записка: !0XXX_DECRYPTION_README.TXT

Email: sergev_petrov1983@mail.ru

Вариант от 28 декабря 2021:

Расширение: .0xxx

Записка: !0XXX_DECRYPTION_README.TXT

Email: alex.uwe.19900978@mail.ru

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

Read to links:

Message + Message + **myMessage**

Write-up, **Topic of Support**

*

Thanks:

Andrew Ivanov (article author)
Michael Gillespie
***
to the victims who sent the samples