HDMR, GO-SPORT

HDMR Ransomware

GO-SPORT Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-128 + RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: dllhost.exe.

Обнаружения:
DrWeb -> Trojan.MulDrop11.25438
BitDefender -> Gen:Win32.FileInfector.guW@aWqkfypi
Malwarebytes -> Ransom.BinADS
Kaspersky -> Trojan.BAT.Agent.aup
TrendMicro -> TROJ_FRS.VSNW19J19
Symantec -> Trojan Horse
Microsoft -> Ransom:Win32/CryptInject!MSR

© Генеалогия: выясняется, явное родство с кем-то не доказано.

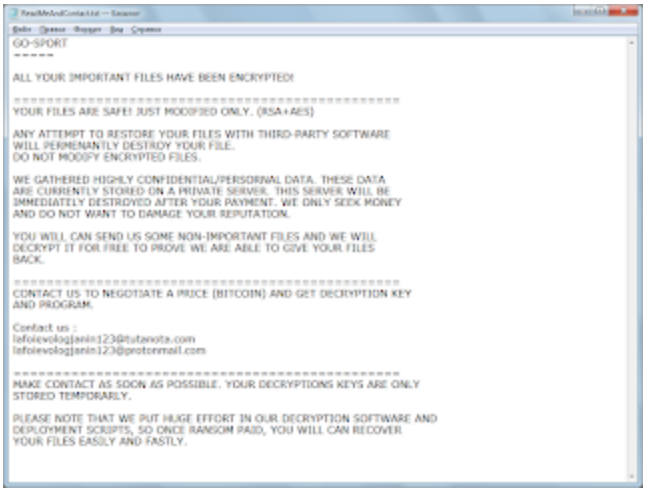
Изображение — логотип статьи

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

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 конец октября 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру. Первые пострадавшие из Франции и Канады.

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



Содержание записки о выкупе:
GO-SPORT
=====
ALL YOUR IMPORTANT FILES HAVE BEEN ENCRYPTED!
==========
YOUR FILES ARE SAFE! JUST MODIFIED ONLY. (RSA+AES)
ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMENANTLY DESTROY YOUR FILE.
DO NOT MODIFY ENCRYPTED FILES.
WE GATHERED HIGHLY CONFIDENTIAL/PERSORNAL DATA. THESE DATA
ARE CURRENTLY STORED ON A PRIVATE SERVER. THIS SERVER WILL BE
IMMEDIATELY DESTROYED AFTER YOUR PAYMENT. WE ONLY SEEK MONEY
AND DO NOT WANT TO DAMAGE YOUR REPUTATION.
YOU WILL CAN SEND US SOME NON-IMPORTANT FILES AND WE WILL
DECRYPT IT FOR FREE TO PROVE WE ARE ABLE TO GIVE YOUR FILES
BACK.
==========
CONTACT US TO NEGOTIATE A PRICE (BITCOIN) AND GET DECRYPTION KEY
AND PROGRAM.

Contact us :
lafoievologjanin123@tutanota.com
lafoievologjanin123@protonmail.com
==========
MAKE CONTACT AS SOON AS POSSIBLE. YOUR DECRYPTIONS KEYS ARE ONLY STORED TEMPORARLY.
PLEASE NOTE THAT WE PUT HUGE EFFORT IN OUR DECRYPTION SOFTWARE AND DEPLOYMENT SCRIPTS, SO ONCE RANSOM PAID, YOU WILL CAN RECOVER YOUR FILES EASILY AND FASTLY.

Перевод записки на русский язык:
GO-SPORT
=====
ВСЕ ВАШИ ВАЖНЫЕ ФАЙЛЫ БЫЛИ ЗАШИФРОВАНЫ!
==========
ВАШИ ФАЙЛЫ В БЕЗОПАСНОСТИ! ТОЛЬКО МОДИФИЦИРОВАНЫ. (РКА + ЭОС)
ЛЮБАЯ ПОПЫТКА ВОССТАНОВИТЬ ВАШИ ФАЙЛЫ С ПОМОЩЬЮ СТОРОННЕЙ ПРОГРАММЫ
УНИЧТОЖИТ ВАШ ФАЙЛ НАВСЕГДА.
НЕ ИЗМЕНЯЙТЕ ЗАШИФРОВАННЫЕ ФАЙЛЫ.
МЫ СОБРАЛИ ОЧЕНЬ КОНФИДЕНЦИАЛЬНЫЕ / ЛИЧНЫЕ ДАННЫЕ. ЭТИ ДАННЫЕ В НАСТОЯЩЕЕ ВРЕМЯ ХРАНЯТСЯ НА ЧАСТНОМ СЕРВЕРЕ. ЭТОТ СЕРВЕР БУДЕТ НЕМЕДЛЕННО УНИЧТОЖАЕТСЯ ПОСЛЕ ОПЛАТЫ. МЫ ТОЛЬКО ИЩЕМ ДЕНЬГИ И НЕ ХОЧУ ВРЕДИТЬ ВАШЕЙ РЕПУТАЦИИ.
ВЫ МОЖЕТЕ ОТПРАВИТЬ НАМ НЕСКОЛЬКО НЕВАЖНЫХ ФАЙЛОВ, И МЫ РАСШИФРУЕМ ИХ БЕСПЛАТНО, ЧТОБЫ ДОКАЗАТЬ, ЧТО МЫ МОЖЕМ ВЕРНУТЬ ВАШИ ФАЙЛЫ.
==========
НАПИШИТЕ НАМ, ЧТОБЫ ДОГОВОРИТЬСЯ О ЦЕНЕ (БИТКОЙН) И ПОЛУЧИТЬ КЛЮЧ РАСШИФРОВКИ
И ПРОГРАММА.
Контакт с нами :
lafoievologjanin123@tutanota.com
lafoievologjanin123@protonmail.com
==========
УСТАНОВИТЕ КОНТАКТ КАК МОЖНО СКОРЕЕ. ВАШИ КЛЮЧИ РАСШИФРОВКИ ТОЛЬКО
ХРАНИТСЯ ВРЕМЕННО.
ОБРАТИТЕ ВНИМАНИЕ, ЧТО МЫ ПРИКЛАДЫВАЕМ ОГРОМНЫЕ УСИЛИЯ В НАШЕЙ ПРОГРАММЕ ДЛЯ РАСШИФРОВКИ И
РАЗВЕРТЫВАНИЕ СЦЕНАРИЕВ, ПОЭТОМУ ПОСЛЕ ВЫКУПА ВЫ СМОЖЕТЕ ВОССТАНОВИТЬ
ВАШИ ФАЙЛЫ ЛЕГКО И БЫСТРО.

Технические детали

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**.

➤ UAC не обходит. Требуется разрешение на запуск.

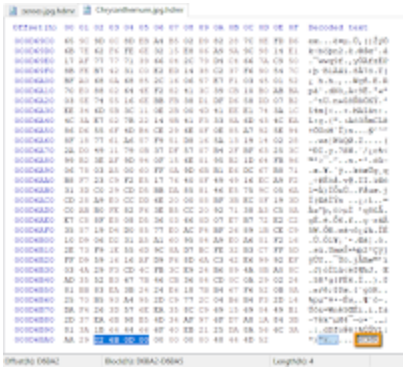
➤ Удаляет теневые копии файлов с помощью команд в BAT-файле.
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin Delete Shadows /all /quiet

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:
ReadMeAndContact.txt
dllhost.exe
<random>.exe - случайное название вредоносного файла

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

➤ Сохраняет исходный размер файла в конце файла и использует маркер "HDMR".



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

Сетевые подключения и связи:
Email: lafoievologjanin123@tutanota.com
lafoievologjanin123@protonmail.com
BTC:
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: **средняя**.
Подробные сведения собираются регулярно. 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 ===

Thanks:

CyberSecurity GrujaRS, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples