GoCryptoLocker

GoCryptoLocker Ransomware

CryptoGoLocker Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем выводит сообщение без требований выкупа. Оригинальное название: goCryptoLocker, CryptoGoLocker, goEncoder. На файле написано: cryptoLocker.exe, main.exe

Обнаружения:
DrWeb -> Trojan.Encoder.31675
BitDefender -> Trojan.GenericKD.33730417
ALYac -> Trojan.Ransom.Filecoder
Avira (no cloud) -> TR/FileCoder.vgssx
ESET-NOD32 -> A Variant Of Win64/Filecoder.BK
Malwarebytes -> Malware.AI.4192834743
Microsoft -> Ransom:Win32/Genasom
Rising -> Ransom.Genasom!8.293 (CLOUD)
Symantec -> Trojan.Gen.2
TrendMicro -> Ransom_Agent.R002C0WJ121

© Генеалогия: Go-вымогатели >> GoCryptoLocker

Изображение — логотип статьи

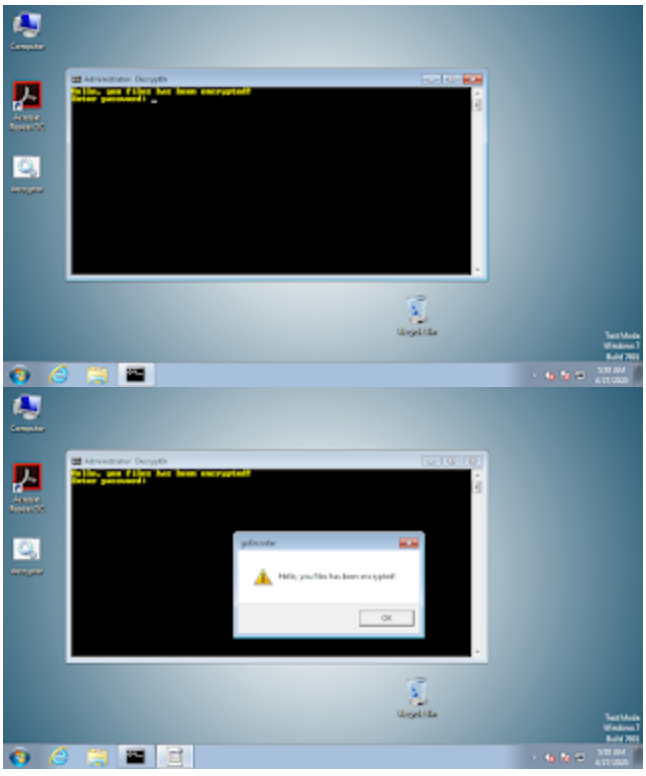
К зашифрованным файлам добавляется расширение: **.GEnc**

GEnc - значит **GoEncoder**, т.к. в диалоговом окне используется название goEncoder.

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

Образец этого крипто-вымогателя был найден во второй половине апреля 2020 г. Но был выложен на github.com примерно на 1-2 месяца раньше. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Запиской с требованием выкупа выступает экран блокировки:



Содержание записки о выкупе:
Hello, you files has been encrypted
Enter password: _

Перевод записки на русский язык:
Привет, твои файлы зашифрованы
Введи пароль: _

Технические детали

После доработки может начать 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 файловых расширений, подвергающихся шифрованию:
.lnk, .png, .jpg, .jpeg, .bmp, .txt, .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pttx
Это документы MS Office, PDF, текстовые файлы, картинки и фотографии, ярлыки программ.

Файлы, связанные с этим Ransomware:
cryptoLocker.exe
main.exe
decryptor.bat
CryptoLocker.bat
<random>.exe - случайное название вредоносного файла

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

\goCryptoLocker\cryptoLocker.exe
%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\CryptoLocker.bat
%USERPROFILE%\Desktop\decryptor.bat

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email:
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: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

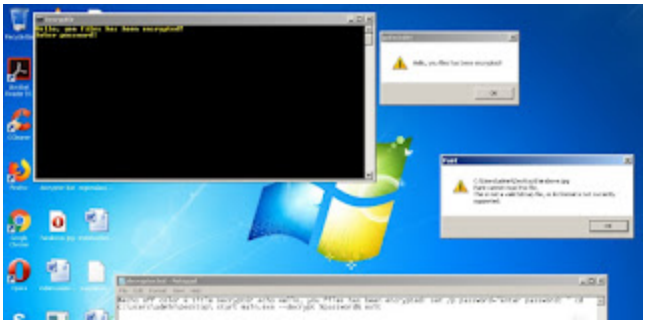
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

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

Обновление от 10 сентября 2020:
Пост в Твиттере >>
Пост в Твиттере >>
Расширение: **.GEnc**

Добавляется в Автозагрузку: C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CryptoLocker.bat
Файлы: main.exe, decryptor.bat, CryptoLocker.bat

➤ Обнаружения:
DrWeb -> Trojan.Encoder.32589
BitDefender -> Trojan.GenericKD.43811587
ESET-NOD32 -> A Variant Of Win64/Filecoder.BK
Malwarebytes -> Ransom.GoCryptoLocker
TrendMicro -> Ransom_Encoder.R002C0WID20

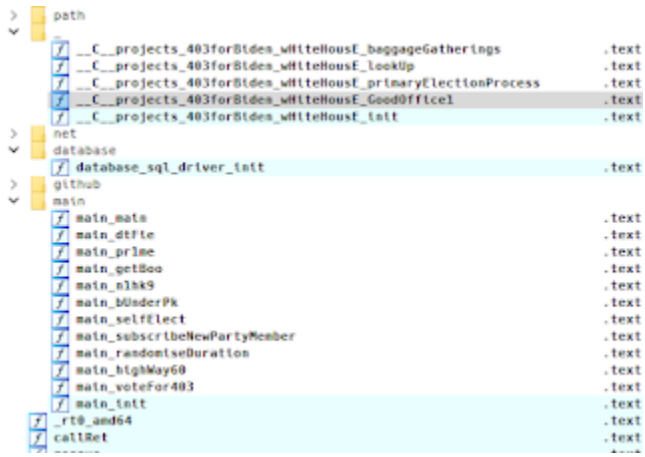


=== 2022 ===

Новый вариант, который называют **HermeticWiper**.
Использует легитимное По EaseUS Partition Master, чтобы повредить разделы.
Сообщение >>
Сообщение >>
Записка: read_me.html
Email: vote2024forjb@protonmail.com, stephanie.jones2024@protonmail.com
Результаты анализов-1: **VT** + **TG**
➤ Обнаружения-1:
DrWeb -> Trojan.Encoder.35007
BitDefender -> Trojan.GenericKD.39061147
ESET-NOD32 -> WinGo/Filecoder.BK
Kaspersky -> Trojan-Ransom.Win64.Agent.dog
Kingsoft -> Win32.PSWTroj.Undef.(kcloud)
Lionic -> Trojan.Win32.Stealer.i!c

Malwarebytes -> Spyware.PasswordStealer
Microsoft -> Ransom:Win32/SonicVote.A!dha
Rising -> Ransom.Agent!1.DC21 (CLOUD)
Symantec -> Trojan Horse
Tencent -> Win32.Trojan.Agent.Gykz
TrendMicro -> Ransom.Win64.GOFILECODER.THBBDBB

Результаты анализов-2: **VT** + **IA**
➤ Обнаружения-2:
BitDefender -> Trojan.GenericKD.39059716
DrWeb -> Trojan.KillDisk.14086
ESET-NOD32 -> A Variant Of Win32/KillDisk.NCV
Kaspersky -> HEUR:Trojan.Win32.HermeticWiper.gen
Lionic -> Trojan.Win32.HermeticWiper.4!c
Malwarebytes -> Trojan.KillDisk
Microsoft -> DoS:Win32/FoxBlade.A!dha
Panda -> Trj/HermeticWiper.A
Rising -> Trojan.HermeticWiper!1.DC1D (CLOUD)
Sophos -> Mal/KillDisk-A
Symantec -> Trojan.KillDisk
TrendMicro -> Trojan.Win32.KILLDISK.SMYECBW



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

Thanks:

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