LV

id-ransomware.blogspot.com/2020/10/lv-ransomware.html

LV Ransomware

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

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: LV. На файле написано: нет данных.

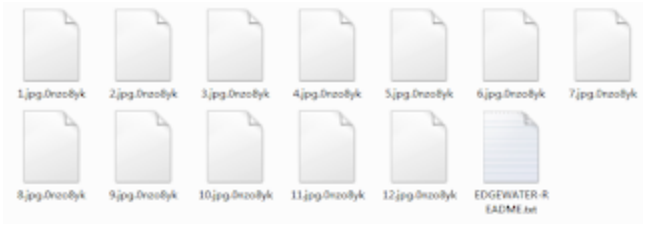
Обнаружения:
DrWeb -> Trojan.Encoder.28004
BitDefender -> Trojan.CryptRedol.Gen.3
ALYac -> Trojan.Ransom.Sodinokibi
Avira (no cloud) -> TR/Dropper.Gen
ESET-NOD32 -> A Variant Of Win32/Filecoder.Sodinokibi.B
Kaspersky -> Trojan-Ransom.Win32.Gen.ybg
Malwarebytes -> Ransom.Sodinokibi
Microsoft -> Ransom:Win32/Revil.SI!MTB
Rising -> Trojan.Generic@ML.93 (RDMK:kLE*
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Filecoder.Efan
TrendMicro -> TrojanSpy.Win32.TRICKBOT.SMC

© Генеалогия: Sodinokibi (REvil) >> LV

Фактически использует код Sodinokibi (REvil) Ransomware. Группировка GOLD NORTHFIELD заменила конфигурацию бета-версии REvil v2.03, чтобы перепрофилировать двоичный файл REvil для LV Ransomware.

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.<random>**
Примеры таких расширений:
.q967a706o
.0nzo8yk



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

Дата создания файла: 24.07.2020. Активность этого крипто-вымогателя была замечена только в октябре-ноябре 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется:
<COMPANY_NAME>-README.txt

Пример такого названия: EDGEWATER-README.txt

Содержание записки о выкупе:

---=== Welcome. Again. ===---

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have 0nzo8yk extension. By the way, everything is possible to recover (restore) but you should follow our instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should visit our website where you can decrypt one file for free. That is our guarantee.

It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. In practice - time is much more valuable than money.

[+] How to get access to our website? [+]

Use TOR browser:

1. Download and install TOR browser from this site: https://torproject.org/
2. Visit our website:

http://4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion

When you visit our website, put the following data into the input form:

Key:

***

!!! DANGER !!!

DON'T try to change files by yourself, DON'T use any third party software or antivirus solutions to restore your data - it may entail the private key damage and as a result all your data loss!

!!! !!! !!!

ONE MORE TIME: It's in your best interests to get your files back. From our side we (the best specialists in this sphere) ready to make everything for restoring but please do not interfere.

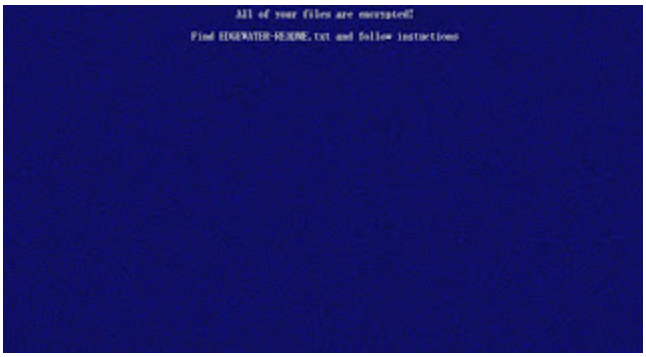
!!! !!! !!

Перевод записки на русский язык:

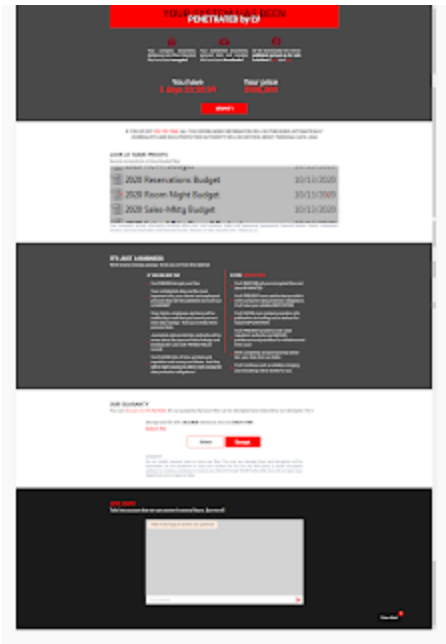
--- === Добро пожаловать. Снова. === ---
[+] Что случилось? [+]
Ваши файлы зашифрованы и теперь недоступны. Вы можете это проверить. Все файлы в вашей системе имеют расширение 0nzo8yk. Кстати, все можно вернуть (восстановить), но вы должны следовать нашим инструкциям. Иначе вы НИКОГДА не сможете вернуть свои данные.
[+] Какие у нас гарантии? [+]
Это просто бизнес и мы заботимся только о получении выгоды. Если мы не выполним свои обязательства, с нами никто не будет иметь дело. Это нас не интересует. Так вы можете проверить возможность восстановления ваших файлов. Для этого вам надо посетить наш сайт, где вы можете бесплатно расшифровать один файл. Это наша гарантия.
Для нас не важно, сотрудничаете вы с нами или нет. Но если вы этого не сделаете, вы потеряете свое время и данные, потому что только у нас есть закрытый ключ для расшифровки ваших файлов. На практике время гораздо дороже денег.
[+] Как получить доступ к нашему сайту? [+]
Используйте браузер TOR:

1. Загрузите и установите браузер TOR с этого сайта: https://torproject.org/
2. Посетите наш веб-сайт:

http://4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion
Когда вы посещаете наш сайт, введите в форму ввода следующие данные:
Ключ:
***
!!! ОПАСНОСТЬ !!!
НЕ ПЫТАЙТЕСЬ изменять файлы самостоятельно, НЕ используйте сторонние программы или антивирусные решения для восстановления ваших данных - это может повлечь за собой повреждение закрытого ключа и, как следствие, потерю всех ваших данных!
!!! !!! !!!
ЕЩЕ РАЗ: в ваших интересах вернуть свои файлы. Со своей стороны мы (лучшие специалисты в этой области) готовы сделать все для восстановления, но не навредите.
!!! !!! !!
Изображение Рабочего стола заменяется на темный фон, аналогичный тому, что ранее использовался в Sodinokibi Ransomware.



Другим информатором жертвы выступает сайт вымогателей, на котором в заголовке используется характерная фраза **YOUR SYSTEM HAS BEEN PENETRATED by LV.** Вероятно, это по замыслу вымогателей должно показать и доказать, что это новые вымогатели, а не те, что ранее использовали Sdinokibi (REvil) для вымогательства денег у пострадавших.



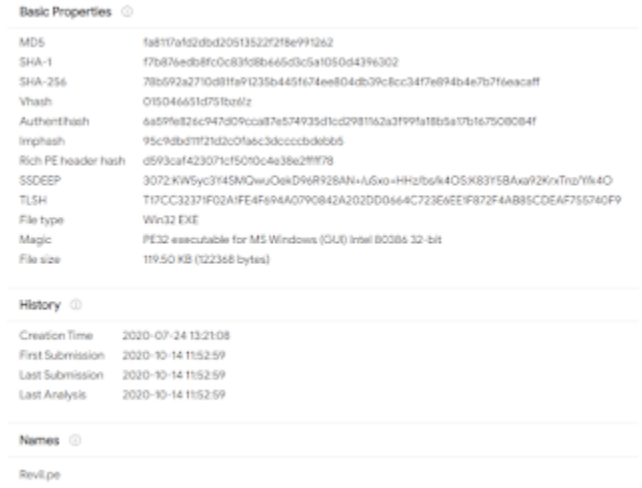
Технические детали

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**.

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:
<ransom_note>.txt - название файла с требованием выкупа
Revil.pe.exe, Revil.pe - название вредоносного файла



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

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

Мьютексы:
Global\530D4C9F-32A8-6FCB-DFF6-A5DE7490E287

Сетевые подключения и связи:
Email:
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
🔻 Triage analysis >>
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >>

⋟ ANY.RUN analysis >>
⧖ **VMRay analysis >>**
Ⓥ VirusBay samples >>
 MalShare samples >>

👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
🔁 JOE Sandbox analysis >>

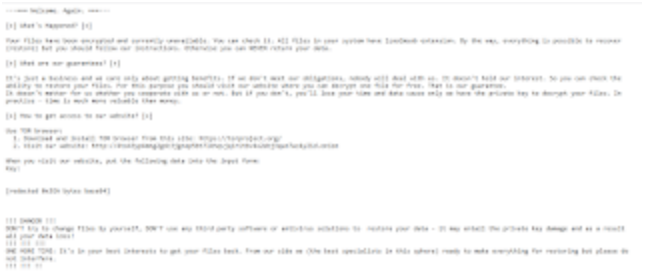
Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

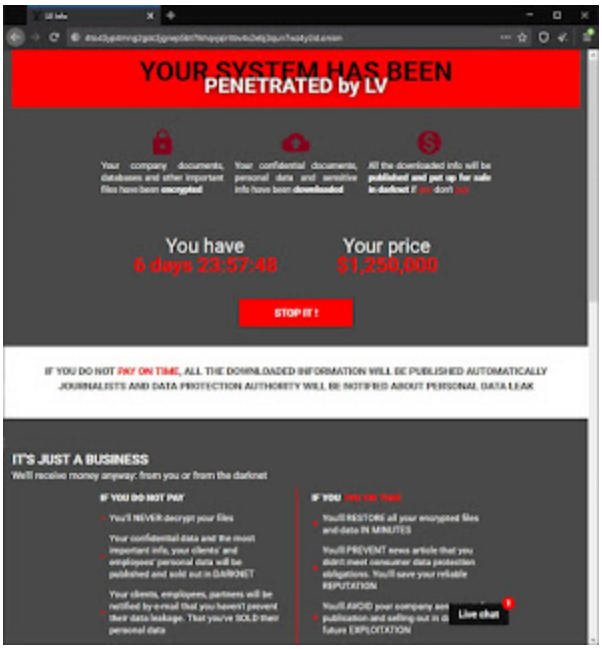
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

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

Обновлеие от 13 ноября 2020:
Пост в Твиттере >>

Записка: 1zoo2msob-README.txt
Tor-URL: xxxx://4to43yp4mng2gdc3jgnep5bt7lkhqvjqiritbv4x2ebj3qun7wz4y2id.onion





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

Read to links:

+ Tweet
ID Ransomware (ID as REvil / Sodinokibi)
Write-up, Topic of Support
Added later: Research by Secureworks (on 22 June, 2021)

Thanks:

Kangxiaopao, Michael Gillespie
Andrew Ivanov (author)
Secureworks
to the victims who sent the samples