BlackCat, ALPHV

id-ransomware.blogspot.com/2021/12/blackcat-ransomware.html

BlackCat Ransomware

ALPHV Ransomware

BlackCat Hand-Ransomware

Aliases: ALPHV-ng, Noberus

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

Этот крипто-вымогатель шифрует данные бизнес-пользователей и корпоративных сетей с помощью комбинации алгоритмов AES-128 (режим CTR) и RSA-2048, а затем требует крупный выкуп в BTC или Monero, чтобы вернуть файлы. Вместо AES может использовать алгоритм ChaCha20. Глобальный открытый ключ, используемый для шифрования локальных ключей, извлекается из файла конфигурации. Оригинальное название: ALPHV-ng RaaS. Используется язык программирования Rust. Может шифровать данные в системах Windows, Linux и VMWare eSXI.

Обнаружения:
DrWeb -> Trojan.Ransom.814
ALYac -> Trojan.Ransom.BlackCat
BitDefender -> Trojan.GenericKD.38153014
ESET-NOD32 -> Win32/Filecoder.OJP
Kaspersky -> UDS:Trojan.Win32.Agentb.a, HEUR:Trojan-Ransom.Win32.BlackCat.gen
Lionic -> Trojan.Win32.BlackCat.j!c
Malwarebytes -> Malware.AI.2115381737, Ransom.FileCryptor
Microsoft -> Trojan:Win32/Woreflint.A!cl
Rising -> Ransom.Blackcat!1.DB0B (CLASSIC)
Symantec -> Ransom.Noberus
Tencent -> Win32.Trojan.Filecoder.Lqor
TrendMicro -> TROJ_GEN.R002H09L321, TROJ_FRS.VSNTLA21, Ransom.Win32.BLACKCAT.YXBLMA

© Генеалогия: предыдущие известные > BlackCat тестовый > BlackCat (ALPHV) > более новые

Этимология названия:

В слове **ALPHV**, без сомнения, скрыто слово ALPHA (альфа). Так вымогатели могли завуалировать первую версию своей вредоносной программы или под ним завуалирован имя (ник) разработчика программы-вымогателя или представителя группы вымогателей. ALPHV-ng - это дальнейшее развитие программы, где ng - Next Generation (англ. следующее поколение).
Для русскоязычного пользователя слово **BlackCat** ("Чёрный кот" или "Чёрная кошка") и картинка в объяснении не нуждаются. Посмотрим насколько у них хватит духа или нюха продолжать этим пользоваться.

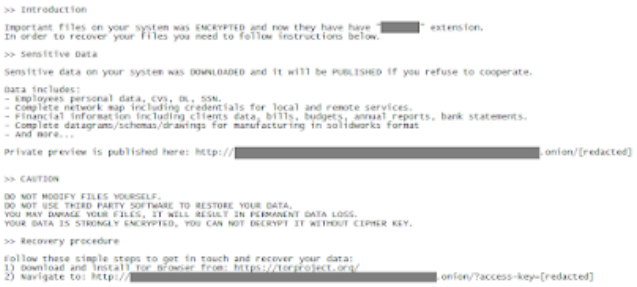
Сайт "ID Ransomware" идентифицирует это как **BlackCat (ALPHV)**.
Информация для идентификации

Активность этого крипто-вымогателя была замечена в середине ноября и во второй половине ноября 2021 г. Тогда использовался более ранний вариант, созданный в начеле ноября 2021. Ориентирован на англоязычных пользователей, может распространяться по всему миру. На сайте утечек названо более 20 организаций из различных секторов и стран, среди них: Австралия, Франция, Германия, Италия, Нидерланды, Филиппины, Испания, Великобритания, США, Багамские острова.

К зашифрованным файлам добавляется настраиваемое семизначное буквенно-цифровое расширение файла. Например, в одном из примеров было расширение: **.sykffle**

Записка с требованием выкупа называется в этом примере: **RECOVER-sykffle-FILES.txt**

Под XXX должно быть добавляемое расширение. Количество знаков может быть любым.


>> Introduction

Important files on your system was ENCRYPTED and now they have have "[redacted]" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

Private preview is published here: http://[redacted].onion/[redacted]

>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://[redacted].onion/?access-key=[redacted]

Содержание записки о выкупе:
» Introduction
Important files on your system was ENCRYPTED and now they have have "sykffle" extension.
In order to recover your files you need to follow instructions below.
» Sensitive Data
Sensitive data on your system was downloaded and it will be published if you refuse to cooperate.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...
Private preview is published here: hxxx://zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd.onion/***
» CAUTION
DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.
» Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torprojoject.org
2) Navigate to: hxxx://mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd.onion/?access-key=***

Перевод записки на русский язык:
» Введение
Важные файлы в вашей системе были зашифрованы и теперь имеют расширение "sykffle".
Чтобы восстановить ваши файлы, вам надо следовать инструкциям ниже.
» Конфиденциальные данные
Конфиденциальные данные из вашей системы были скачаны и будут опубликованы, если вы откажетесь от сотрудничества.
Данные включают:
- Персональные данные сотрудников, резюме, DL, SSN.
- Полная карта сети, включая учетные данные для локальных и удаленных служб.
- Финансовая информация, включая данные клиентов, счета, бюджеты, годовые отчеты, банковские выписки.
- Полные датаграммы / схемы / чертежи для производства в формате solidworks
- И больше...
Приватный превью опубликован здесь: http://***.onion/***
" ОСТОРОЖНО
НЕ ИЗМЕНЯЙТЕ ФАЙЛЫ САМОСТОЯТЕЛЬНО.
НЕ ИСПОЛЬЗУЙТЕ ПРОГРАММЫ ТРЕТЬИХ СТОРОН ДЛЯ ВОССТАНОВЛЕНИЯ ДАННЫХ.
ВЫ МОЖЕТЕ ПОВРЕДИТЬ СВОИ ФАЙЛЫ, ЭТО ПРИВЕДЕТ К ПОСТОЯННОЙ УТЕЧКЕ ДАННЫХ.
ВАШИ ДАННЫЕ НАДЕЖНО ЗАШИФРОВАНЫ, ВЫ НЕ МОЖЕТЕ РАСШИФРОВАТЬ ИХ БЕЗ КЛЮЧА ШИФРОВАНИЯ.
» Процедура восстановления
Выполните следующие простые шаги, чтобы связаться и восстановить свои данные:
1) Загрузите и установите Tor Browser с сайта: https://torprojoject.org
2) Перейдите по адресу: http://***.onion/?access-key=***
Неполный скриншот одного из сайтов вымогателей:

Технические детали + IOC

Рекламируется с начала декабря 2021 на двух подпольных русскоязычных форумах киберандеграунда (XSS и Exploit). Приглашаются пентестеры, операторы и участники других вымогательситк проектов. Аффилированным партнерам обещается доход в размере от 80% до 90% от полученного выкупа.

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**.

➤ Во время проведения атаки ALPHV используется PowerShell для изменения параметров безопасности Защитника Windows во всей сети жертвы, а также запускается двоичный файл программы-вымогателя, интерактивный процесс, на нескольких хостах с помощью PsExec.
➤ Удаляет теневые копии файлов и моментальные снимки ESXi для предотвращения восстановления.
➤ Использует команду для сбора универсальных уникальных идентификаторов (UUID) с зараженных машин. Затем UUID и параметр "токен доступа" используются для генерации «ACCESS_KEY». Подробнее в статье Symantec >>
➤ Используется CryptGenRandom для генерации ключей шифрования.

Детали шифрования:
В автоматическом режиме BlackCat проверяет наличие аппаратной поддержки алгоритма AES (есть во всех современных процессорах) и использует её. Если нет поддержки AES, то BlackCat шифрует файлы с помощью алгоритма ChaCha20.

Список типов файлов, подвергающихся шифрованию:
Почти все типы файлов, кроме тех, что находятся в списках исключений.
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Список пропускаемых расширений:
.386, .adv, .ani, .bat, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepacJc, .diagcab, .diagcfg, .diagpkg, .dll, .drv, .exe, .hip, .hta, .icl, .ico, .ics, .idx, .iens, .key, .ldf, .lnk, .lock, .mod, .mpa, .msc, .msi, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .pdb, .prf, .psl, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx (50 расширений).

Список завершаемых процессов и служб:
agntsvc, backup, dbeng50, dbsnmp, encsvc, excel, firefox, infopath, isqlplussvc, memtas, mepocs, msaccess, msexchange, mspub, mydesktopqos, mydesktopservice, notepad, ocautoupds, ocomm, ocssd, onenote, oracle, outlook, powerpnt, sqbcoreservice, sql*, sql, sql, steam, svc$, synctime, tbirdconfig, thebat, thunderbird, veeam, visio, vss, winword, wordpad, xfssvccon,

Список пропускаемых директорий:
All users, Appdata, Application data, Boot, Config.msi, Default, Google, Intel, Mozilla, Msocache, Perflogs, Program files (x86), Program files, ProgramData, Public, Recycle.bin, System volume information, Tor browser, Windows.~ws, Windows, Windows.~bt, Windows.old

Список пропускаемых файлов:
autorun.inf, boot.ini, bootfont.bin, bootsect.bak, desktop.ini, iconcache.dbn, nthumbs.dbn, ntldr, ntuser.dat, ntuser.dat.log ntuser.ini

Маркер файлов:

19 47 B7 4D в конце зашифрованного файла и перед зашифрованным ключом, который представляет собой JSON с некоторыми настройками.

Файлы, связанные с этим Ransomware:
RECOVER-sykffle-FILES.txt - название файла с требованием выкупа;
RECOVER-sykffle-FILES.txt.png - изображение, заменяющее обои Рабочего стола;

DllHost.exe, keller.exe, 3ddxzjjjn.dll - названия вредоносного файла.

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

C:\Users\User\AppData\Local\Temp\3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83.exe

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL (примеры): hxxx://zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd.onion/b21***
hxxx://mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd.onion/***
Для каждой новой атакованной компании создается новый onion-домен.
Email: -
BTC: -

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

MD5: aea5d3cced6725f37e2c3797735e6467
SHA-1: 087497940a41d96e4e907b6dc92f75f4a38d861a
SHA-256: 3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83
Vhash: 0260876d15755c0d5d1d10c8z73210301hz15zf7z
Imphash: 2c3e267ae163c15bfc251e74ea5319b2

Некоторые другие образцы можно найти на сайте BA:
https://bazaar.abuse.ch/browse/tag/blackcat/

Степень распространённости: **высокая**.
Информация дополняется. Присылайте образцы.

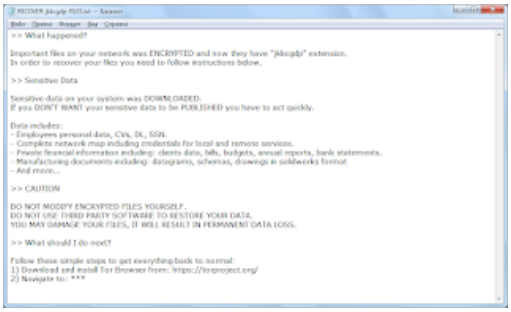
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

Три года назад и ещё раз не так давно мы уже видели, как кто-то использовал название BlackCat Ransomware. Но тогда это активно не распространялось или проходило тестирование, поэтому не попало в наш Дайджест. На момент написания статьи никто не доказал и не опроверг связь сегодняшего BlackCat Ransomware с предыдущими.

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

Вариант от 30 декабря 2021:
Сообщение на форуме >>

Расширение: **.jkkcgdp**
Записка: RECOVER-jkkcgdp-FILES.txt



=== 2022 ===

Новость от 4 февраля 2022:
Краткое содержание интервью, данное аналитику Recorded Future Дмитрию Смилянцу представилем группы вымогателей из BlackCat (ALPHV).

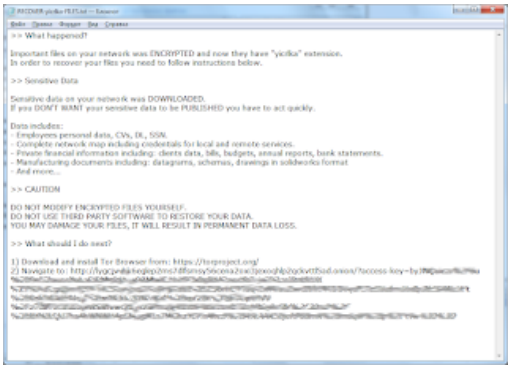
ALPHV: Наше единственное имя - ALPHV. BlackCat был изобретен компанией The Record, а BC.a Noberus — компанией Symantec.

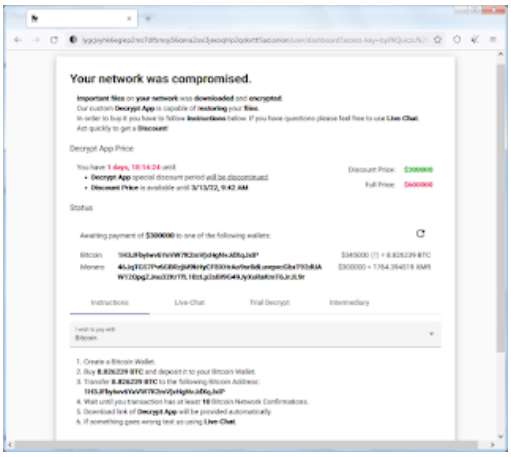
✋ **Уточнение:** Название BlackCat впервые использовано исследователем MalwareHunterTeam в Твиттере **и сразу же опубликовано здесь**, в Дайджесте, в этот статье. **Все остальные публикации вторичны.**

ALPHV: ...Нет никакого ребрендинга или смешения талантов, потому что мы не имеем прямого отношения к партнерским программам GandCrab/REvil, BlackMatter/DarkSide, Maze/Egregor, Lockbit и прочим. Мы позаимствовали их достоинства и устранили их недостатки.
...Мы без преувеличения считаем, что на данный момент на рынке нет конкурентоспособного нам программного обеспечения. Помимо качественного софта, для продвинутых партнеров мы предоставляем полный спектр услуг, связанных с выкупом — метавселенную или премиум-обслуживание. Мы в другой весовой категории, поэтому никого не признаем и не будем делать вымогательские дома TikTok.
...Мы абсолютно не заинтересованы ни в каком сотрудничестве, расширении или взаимодействии с другими филиалами и работаем только с русскоязычными партнерами. Недавно была первая чистка, скоро будет вторая и мы закроемся. Географически расширяться не планируем, но обязательно добавим китайский язык после арабского... :)
...Язык программирования RUST выбран как современный кроссплатформенный ЯП низкого уровня. В консольной команде имя проекта alphv-N(ext)G(eneration). Мы сделали действительно новый продукт, с новым внешним видом и подходом, отвечающим современным требованиям как к RaaS-решению, так и к высококлассному коммерческому ПО.
...Мы не нападаем на госмедучреждения, машины скорой помощи, больницы. Это правило не распространяется на фармацевтические компании, частные клиники.
...Наша главная цель — создать собственную метавселенную RaaS, включающую в себя весь спектр услуг, связанных с нашим бизнесом.

Новость от 5 февраля 2022:
BleepingComputer сообщает, что некоторые специалисты выявили совпадения в действиях предыдущих вымогателей BlackMatter/DarkSide и BlackCat/ALPHV.
Ссылка на статью >>

Вариант от 11 марта 2022:
Сообщение >>
Расширение: **.yicrlka**
Записка: RECOVER-yicrlka-FILES.txt





Bitcoin: 1H3JFbyiwv6YeVW7K2mVjxHgNvJdXqJxiP
Monero:
46JqTG57Pv6GBRzjM9kHyCF8XHrAo9sr8dLuvqwcGbxT92dUAW12QpgZJnu32KrTfL1BzLp2sBi9G49JyXuRaKmT6JrJL9r

Вариант от 15 марта 2022:
Сообщение >>
Файл: alpha.exe
Результаты анализов: **VT**

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

Read to links:

Message + Message + **myMessage**
Write-up, Write-up, Topic of Support
Added later: Write-up by Symantec

Added later: Write-up, Write-up, Write-up, Write-up, Write-up

Thanks:

MalwareHunterTeam, SAJID HASSAN
Andrew Ivanov (article author)
to authors of the newer researches
to the victims who sent the samples