HelloKitty, Kitty

id-ransomware.blogspot.com/2020/11/hellokitty-ransomware.html

HelloKitty Ransomware

Kitty Ransomware

HelloKitty Hand-Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES-256 и RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: ag.exe. Написан на C++. В мае 2021 появился новый вариант написанный на языке Go.
Существует несколько разных версий, которые используют для шифрования разную комбинацию алгоритмов: AES-256 + RSA-2048, AES-128 + NTRU. Также есть версия для Linux, использующая AES-256 + ECDH.

Обнаружения:
DrWeb -> Trojan.Encoder.33143, Trojan.Encoder.33348, Trojan.Encoder.33464
BitDefender -> Gen:Heur.Ransom.Imps.1, Gen:Variant.Ransom.Adhubllka.1
ALYac -> Trojan.Ransom.Filecoder
Avira (no cloud) -> TR/Redcap.pdjtm, HEUR/AGEN.1127999
ESET-NOD32 -> A Variant Of Win32/Filecoder.DeathRansom.D
Kaspersky -> HEUR:Trojan-Ransom.Win32.Encoder.gen
Malwarebytes -> Ransom.DeathRansom
Microsoft -> Trojan:Win32/Ymacco.AA9A
Rising -> Trojan.Generic@ML.85 (RDML:Hg3*
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Trojan.Win32.IMPS.USMANKI20

© Генеалогия: ✂️ DeathRansom, Adhubllka > TechandStrat > HelloKitty (Kitty) > FiveHands
© Генеалогия: HelloKitty (Kitty) > Kitty Go, Kitty Linux


Изображение — логотип статьи

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

Этимология названия:
Слово **HelloKitty** есть в мьютексе **HelloKittyMutex**. Вымогатели оказались настолько пугливыми, что не воспользовались email для связи с жертвами, использовали только специальный адрес на onion-сайте, без первичной страницы домена, никак не назвали свою программу и напуганные вопросами в чате сразу сбежали восвояси. Поэтому в логотип статьи был добавлен напуганный котенок.

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 середину ноября 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **read_me_lkdtt.txt**
Вероятно, что используется шаблон: **read_me_<abbreviation>.txt**

Содержание записки о выкупе:

Hello dear user.
Your files have been encrypted.
-- What does it mean?!
Content of your files have been modified. Without special key you can't undo that operation.
-- How to get special key?
If you want to get it, you must pay us some money and we will help you.
We will give you special decryption program and instructions.
-- Ok, how i can pay you?
1) Download TOR browser, if you don't know how to do it you can google it.
2) Open this website in tor browser:
hxxx://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion/02f6af250649555ea1b65f20fd9e815b23ba7d84829b93e6d8dbdb1
3) Follow instructions in chat.

Перевод записки на русский язык:
Привет дорогой пользователь.
Ваши файлы зашифрованы.
-- Что это значит?!
Содержание ваших файлов было изменено. Без специального ключа вы не сможете отменить эту операцию.
- Как получить специальный ключ?
Если вы хотите его получить, вы должны заплатить нам немного денег, и мы вам поможем.
Мы дадим вам специальную программу расшифровки и инструкции.
- Хорошо, как я могу тебе заплатить?
1) Загрузите браузер TOR, если не знаете, как это сделать, можете погуглить.
2) Откройте этот веб-сайт в браузере TOR:
hxxx://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion/02f6af250649555ea1b65f20fd9e815b23ba7d84829c93db10f8d8d8
3) Следуйте инструкциям в чате.

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**.
➤ При выполнении HelloKitty завершает 1706 процессов, закрывает 57 служб и удаляет теневые копии файлов.

➤ HelloKitty содержит встроенный открытый ключ RSA-2048. Этот открытый ключ хешируется SHA256 и используется в качестве идентификатора жертвы в записке с требованием выкупа. Этот открытый RSA-ключ также используется для шифрования симметричного ключа каждого файла.
Для симметричного ключа HelloKitty генерирует 32-байтовое начальное значение на основе метки времени ЦП. Генерируется ключ Salsa20, который шифрует второе 32-байтовое начальное значение. Зашифрованный результат подвергается операции XOR с первым семенем, в результате чего получается 32-байтовый ключ, используемый для AES-шифрования каждого файла.
После того, как каждый файл зашифрован, исходный размер файла, магическое значение DE C0, AD BA и ключ AES зашифровываются с помощью открытого ключа RSA и добавляются к файлу. HelloKitty добавляет эти дополнительные метаданные в зашифрованный файл. Затем он добавляет четыре магических байта DA DC CC AB в конец зашифрованного файла.
В зависимости от версии HelloKitty может изменять или не изменять расширение файла.
В других образцах HelloKitty вместо RSA использовался встроенный открытый ключ NTRU.

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:
read_me_lkdtt.txt - название файла с требованием выкупа
ag.exe - случайное название вредоносного файла

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

C:\Users\Admin\AppData\Local\Temp\ag.exe

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

Мьютексы:
HelloKittyMutex
Мьютекс нужен, чтобы предотвратить запуск нескольких экземпляров шифровальщика одновременно.

Сетевые подключения и связи:
Tor-URL: hxxx://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion

Email: -
BTC: -
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ 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.

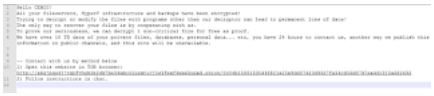
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

DeathRansom Ransomware - ноябрь 2019 - август 2020
другие варианты - в течении 2020
TechandStrat Ransomware - октябрь 2020
HelloKitty Ransomware - ноябрь 2020
FiveHands Ransomware - декабрь 2020 - январь 2021 и далее

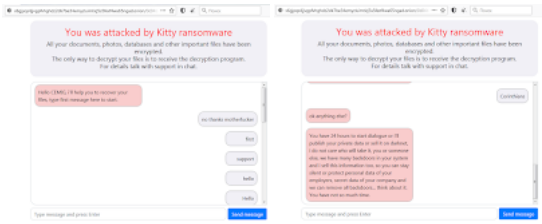
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Вариант от 26-27 декабря 2020:
Сообщение >>
Нацелен на бразильские компании.
В тексте упоминаеттся CEMIG - бразильская энергетическая компания.

Расширение: **.kitty**
Записка: read_me_lkdtt.txt



➤ Другим информатором является чат на Tor-сайте.
Немного текста от вымогателей:



You was attacked by Kitty ransomware
All your documents, photos, databases and other important files have been encrypted.
The only way to decrypt your files is to receive the decryption program.
For details talk with support in chat.
Hello CEMIG, i'll help you to recover your files, type first message here to start.
***
You have 24 hours to start dialogue or i'll publish your private data or sell it on darknet, i do not care who will take it, you or someone else, we have many backdoors in your system and i sell this information too, so you can stay silent or protect personal data of your employers, secret data of your company and we can remove all backdoors... think about it. You have not so much time.

➤ Обнаружения:
DrWeb -> Trojan.Encoder.33348
Avira (no cloud) -> HEUR/AGEN.1127999
BitDefender -> Gen:Variant.Ransom.Adhubllka.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.DeathRansom.D
Kaspersky -> HEUR:Trojan.Win32.Udochka.gen
Malwarebytes -> Ransom.DeathRansom
Rising -> Trojan.Generic@ML.97 (RDML:Xr*
Symantec -> Ransom.CryptoTorLocker
Tencent -> Win32.Trojan.Filecoder.Wpti
TrendMicro -> TROJ_GEN.R002H09LR20, Ransom_CryptoLocker.R002C0DG821

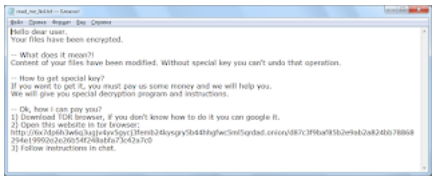
Вариант от 25-26 декабря или позже, в январе 2021:
Отдельная статья: FiveHands Ransomware >>
Расширение: **.crypt**
Записка: DECRYPT_NOTE.txt
Имеются отличия, см. сравнительную таблицу разных функций для FiveHands - HelloKitty - DeathRansom.

Feature	FIVEHANDS	HELLOKITTY	DEATHRANSOM
Programming Language	C++	C++	C
Symmetric Encryption	AES 128	AES 256	AES 256
Asymmetric Encryption	Embedded NTRU Key	Embedded RSA or NTRU Key	Curve25519 ECDH and RSA key creation
Same directory and file name exclusions	No	Yes	Yes
Accepts CLI Arguments	Yes	No	No
Network Connections	No	No	Yes
Locale Check	No	No	Yes
Mutex Check	No	Yes	No
Bytes Appended to Encrypted Files	DB DC CC AB	DA DC CC AB	AB CD EF AB

=== 2021 ===

Вариант от 28 января 2021:

Сообщение >>
Расширение: .crypted
Записка: read_me_lkd.txt
Tor-URL: hxxx://6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad.onion/*
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33464
BitDefender -> Generic.Malware.PfVPk!12.299C21F3
ESET-NOD32 -> A Variant Of Win32/Filecoder.DeathRansom.C
Kaspersky -> HEUR:Trojan.Win32.AntiAV
Malwarebytes -> Ransom.HelloKitty
Microsoft -> Ransom:Win32/Death.DB!MTB
Rising -> Ransom.Death!8.11553 (CLOUD)
Symantec -> Trojan.Gen.MBT
Tencent -> Win32.Trojan.Filecoder.Ecav
TrendMicro -> Ransom.Win32.DEATHRANSOM.F



Вариант от 9 февраля 2021:

Отдельная статья: **Epically Ransomware >>**

Обновление от 11 февраля 2021:
Некоторые пояснения по вариантам HelloKitty:

Статья на сайте Emsisoft >>

Вариант от 9 мая 2021:
Название: Kitty Go.
Сообщение >>
Объект атаки: медицинская компания Western Pathology (США).
Расширение: .crypted
Записка: read_me_unlock.txt
Новый проект: /Go/src/kitty/kidata/kidata.go

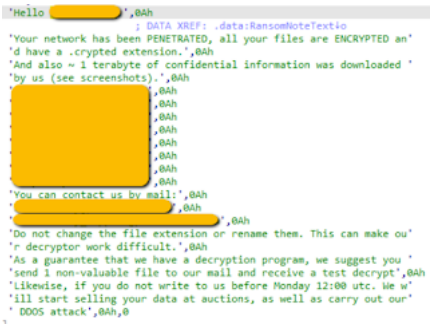
➤ Содержание записки:
Hello dear westernpathologyinc!
Unfortunately, your files have been encrypted and attackers are taking over 1 TB of your personal data.
financial reports and many other documents.
Do not try to recover files yourself, you can damage them without special software.
We can help you recover your files and prevent your data from leaking or being sold on the darknet.
Just contact support using the following methods and we will decrypt ..one non-important file for free to convince you of our honesty.
use TOR browser to talk with support
hxxx://uqudwxzszbcj6uxbhbdccmixvwjfewn565ifotzvcbbimsjjcczsvpyd.onion/*

Результаты анализов: **VT** + **VT** + **VMR** + **JSB** + **IA** + **IA** + **IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33894
BitDefender -> Trojan.Ransom.Agent.BX
ESET-NOD32 -> A Variant Of WinGo/Filecoder.M
Kaspersky -> VHO:Trojan-Ransom.Win32.Convagent.gen
Malwarebytes -> Malware.AI.4199637328
Microsoft -> Trojan:Win32/Hynamer.C!ml
Rising -> Ransom.Encoder!8.FFD4 (RDMK:cmR*

TrendMicro -> TROJ_GEN.R002H07E921, Ransom_Encoder.R002C0WEC21
Вариант от даты появления:
Название: Kitty Linux (для Linux-систем)

Расширение: **.crypt**
Используется OpenSSL (AES256 + secp256k1 + ECDSA)

Вариант июня 2021:
Сообщение >>
Название: Vice Society. Вероятно спин-офф от HelloKitty.
Шифрует системы Windows и Linux с помощью OpenSSL (AES256 + secp256k1 + ECDSA).
Расширение: **.v-society**



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

Read to links:

Message + Message
ID Ransomware (ID as HelloKitty)
Write-up, **Topic of Support**
Added later: Write-up by FireEye (on April 29, 2021)

Thanks:

Andrew Ivanov (article author)
quitman7, Michael Gillespie
FireEye
to the victims who sent the samples