Шифровальщики-вымогатели The Digest "Crypto-Ransomware"

id-ransomware.blogspot.com

Kekpop

Kekpop Ransomware

Aliases: Kekware

Variants: YourCyanide

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует выкуп $500 в BTC, чтобы вернуть файлы. Оригинальное название: Kekpop. На файле написано: kekpop.cmd.

Обнаружения:
DrWeb ->
ALYac -> Trojan.BAT.Agent
BitDefender -> Trojan.GenericKD.50265580
ESET-NOD32 -> A Variant Of Generik.LKONBMI
Kaspersky -> HEUR:Trojan.BAT.Generic
Malwarebytes ->
Microsoft ->
Rising ->
Tencent -> Bat.Trojan.Generic.Ebzs
TrendMicro ->

© Генеалогия: ??? >> Kekpop

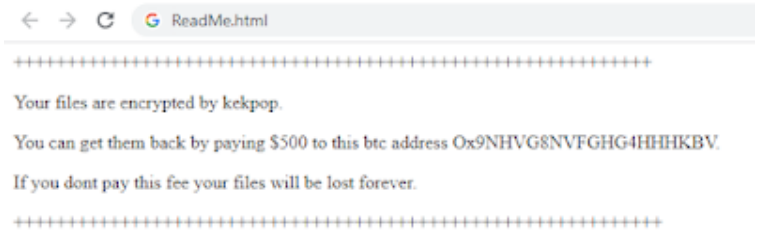
IDR IDENTIFIED

Сайт "ID Ransomware" это пока не идентифицирует.
Информация для идентификации

Активность этого крипто-вымогателя была в начале мая 2022 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

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

Записка с требованием выкупа называется: **ReadMe.html**



Содержание записки о выкупе:
++
Your files are encrypted by kekpop.
You can get them back by paying $500 to this btc address Ox9NHVG8NVFGHG4HHHKBV.
If you dont pay this fee your files will be lost forever.
++

Перевод записки на русский язык:
Ваши файлы зашифрованы kekpop.
Вы можете получить их обратно, заплатив $500 на этот биткойн-адрес Ox9NHVG8NVFGHG4HHHKBV.
Если вы не заплатите эту плату, ваши файлы будут утеряны навсегда.

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

Технические детали + IOC

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.

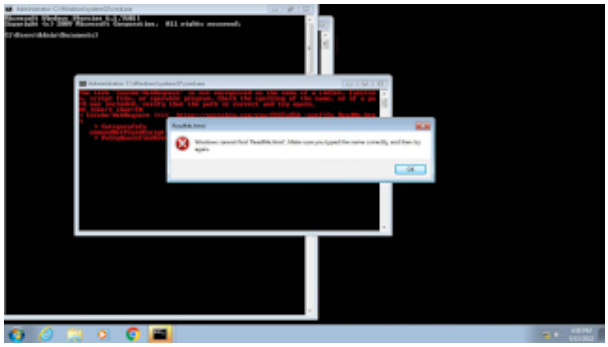
Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

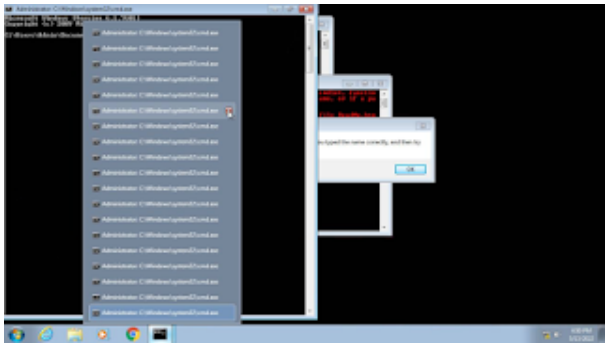
➤ Использует технологии Microsoft: CMD и PowerShell для атаки.

Список типов файлов, подвергающихся шифрованию:
Это могут быть документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
ReadMe.html - название файла с требованием выкупа;
kekpop.cmd - название вредоносного файла;
black.bat - простой командный файл;
GetToken.exe - вредоносный файл, загружаемый через Discord;
ps1-файлы.

Проект вымогателя недоработан, множество окон с командами, это видно на скриншотах.





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

hxxxs://cdn.discordapp.com/attachments/971160786015772724/971191444410875914/GetToken[.]exe

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: -
BTC: Ox9NHVG8NVFGHG4HHHKBV (ненастоящий)

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

MD5: f190183b6a6f55daa406c25cf5da66d8
SHA-1: 89168542e0cec21bbafeafe39361994194576f61
SHA-256: ea81248fddbf9080018845bf7862b9ceb8ab942526c1adcf20030f043c57ad99

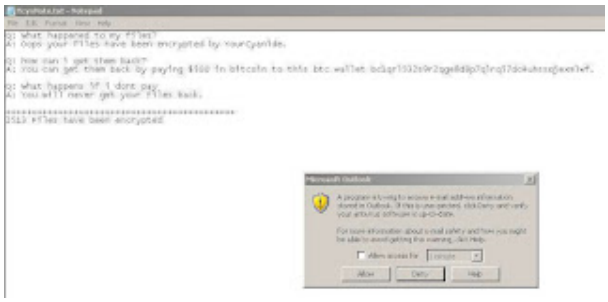
Степень распространённости: низкая.
Информация дополняется. Присылайте образцы.

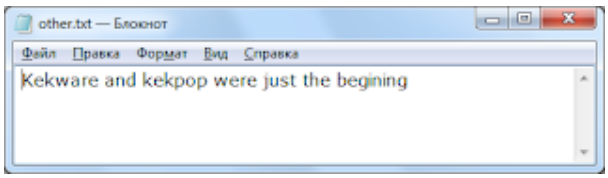
=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

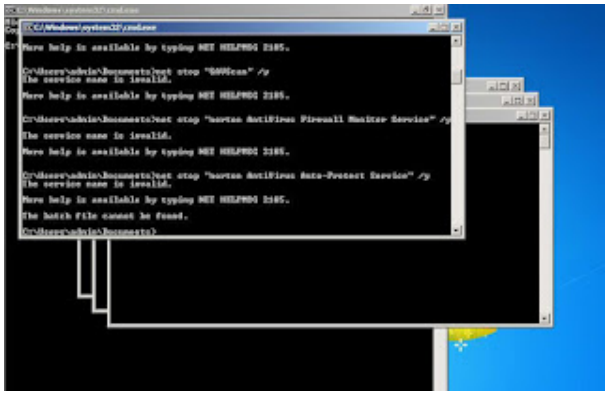
=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Вариант от 15 мая 2022:
Сообщение >>

Мое сообщение >>
Расширение: **<random>.cyn**
Записки: YcynNote.txt, other.txt
Email: yourcyanide.help@gmail.com
Файлы: YourCyanide.cmd, 1.cmd, ycynlog.cmd
Результаты анализов: **VT** + **AR**
Обнаружения:
BitDefender -> Gen:Heur.Bat.1
DrWeb -> BAT.Siggen.179
Kaspersky -> HEUR:Trojan.BAT.Generic
Microsoft -> Trojan:Script/Wacatac.B!ml
Symantec -> Trojan.Gen.MBT
Tencent -> Bat.Trojan.Generic.Svgz







С помощью командного файла KillAVS.bat вырубает следующие защитные функции и антивирусные службы:
Ahnlab Task Scheduler, AntiSpyware, AntiVirus Auto Protect Service, AntiVirus Client, AntiVirus Corporate Edition, AntiVirus Firewall Monitor Service, AntiVirus Server, Automatic Updates, ccEvtMGR, ccPwdSvc, ccSetMGR, cls, Core LC, DefWatch, ERSvc, eTrust Antivirus Job Server, eTrust Antivirus Realtime Server, eTrust Antivirus RPC Server, eventlog, helpsvc, InoRPC, InoRT, InoTask, McShield, mcupdmgr.exe, MonSvcNT, MpfService, MskService, NAV Alert, Nav Auto-Protect, navapsvc, netsvcs, Network Drivers Service, NProtectService, PC-cillin Personal Firewall,

Personal Firewall Service, SAVScan, Security Center, SecurityCenter Update Manager, Serv-U, Sophos Anti-Virus, Sophos Anti-Virus Network, Spamkiller Server, SPBBCSvc, spoolnt, srservice, Sygate Personal Firewall Pro, SyGateService, Trend Micro Proxy Service, Trend NT Realtime Service, Unerase Protection, ViRobot Professional Monitoring, VirusScan Online Realtime Engine, vrmonsvc
---
Еще варианты: файлы YourCyanide.cmd, YourCyanide_obf.bat

Результаты анализов: **VT** + **TG** / **VT** + **TG**

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

Thanks:

```
Petrovic
Andrew Ivanov (article author)
***
to the victims who sent the samples
```


RansomHouse

RansomHouse Extortion Group

RansomHouse Hacking Team

RansomHouse Ransomware

(хакеры-вымогатели, доксеры, публикаторы) (первоисточник)
Translation into English

Эти хакеры-вымогатели на своем сайте сообщают, что сами они не атакуют ресурсы бизнес-пользователей, не похищают и не шифруют данные, чтобы затем требовать выкуп в биткоинах за возврат слитых файлов, не опубликовав их для всеобщего обозрения. Они называют себя посредниками, предпочитая мирные соглашения со сторонами. Правда ли это, мы не знаем. В любом случае, посредники, заинтересованные в уплате выкупа, состоят в сговоре с другими хакерами, которые атакуют и требуют выкуп за возврат файлов в прежнее состояние.
Оригинальное название группы этих посредников: RansomHouse. Само слово "Ransom" подразумевает "выкуп", странно, что они выбрали себе такое название, но называют себя посредниками между хакерами, укравшими данные и тем, у кого эти данные увели. Такие странности имеют название — "оговорка по Фрейду". Назвались бы MediationHouse, тогда и были бы посредниками. Впрочем, значок биткоина в логотипе вымогателей и сумма оплаты в 1 биткоин, говорят о том, что эти люди **точно вымогатели**, как бы они сами себя не называли.

Обнаружения:
Не образцов используемого вредоносного ПО.

© Генеалогия: ??? >> RansomHouse

Сайт "ID Ransomware" это пока не идентифицирует.
Информация для идентификации

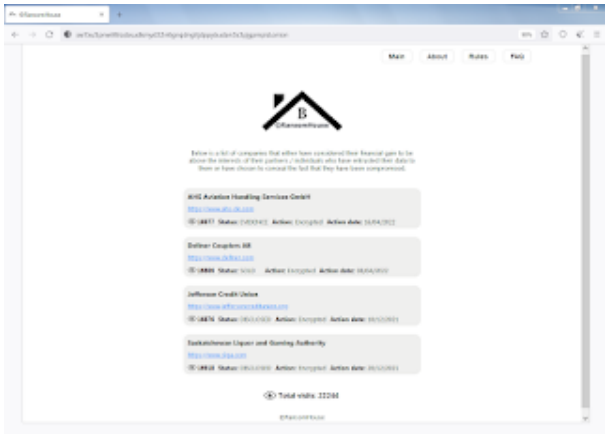
Информация о первых пострадавших от вымогателей размещена в декабре 2021 г. на сайте группы RansomHouse. Сайт на английском языке, значит они ориентированы на англоязычные компании и могут быть активны по всему миру.

Добавляемое к зашифрованным файлам расширение видимо зависит от названия атакованного ресурса компании или её названия. Сами RansomHouse к этому отношения не имеют.

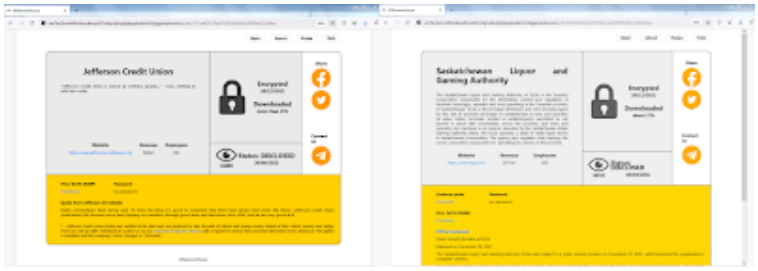
Пример записки и образец вредоносного файла получить не удалось.

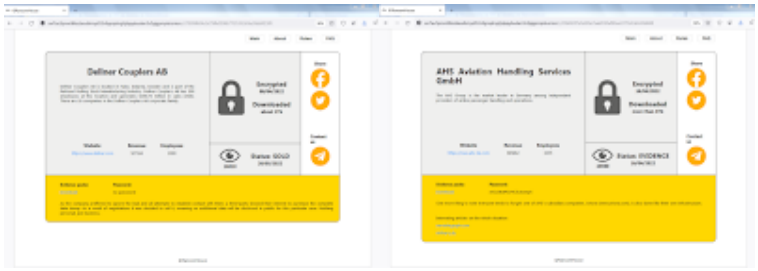
По аналогии с другими статьями о хакерах-вымогателях, мы решили опубликовать текст с сайта группы RansomHouse, чтобы рассказать о том, что они собой представляют и как себя позиционируют.

Страница "Main"



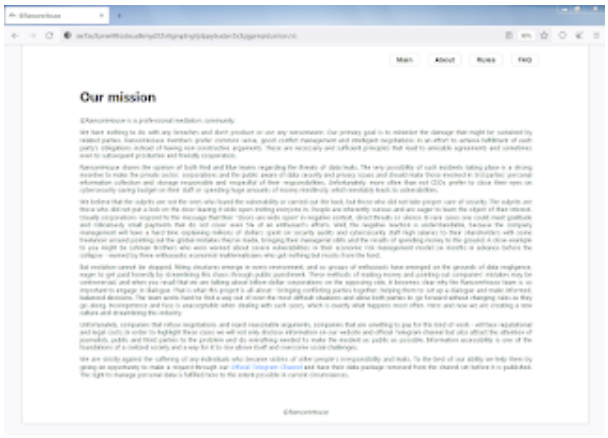
Содержание:
Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.
AHS Aviation Handling Services GmbH
Dellner Couplers AB
Jefferson Credit Union
Saskatchewan Liquor and Gaming Authority





Краткий перевод:
Ниже есть список компаний, поставивших свою финансовую выгоду выше интересов своих партнеров/лиц, доверивших им свои данные, либо пожелавших скрыть факт компрометации.
***

Страница "About"



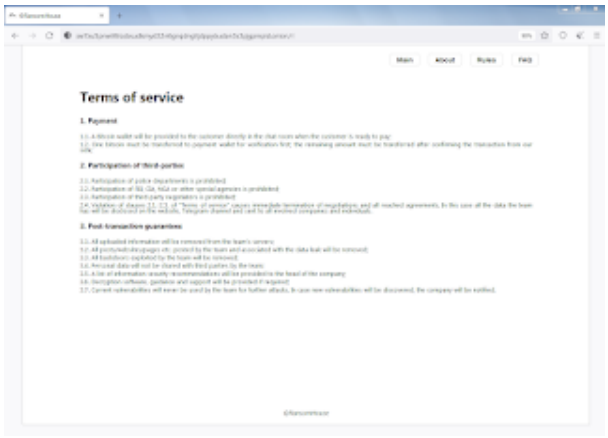
Содержание:
Our mission
©RansomHouse is a professional mediators community.
We have nothing to do with any breaches and don't produce or use any ransomware. Our primary goal is to minimize the damage that might be sustained by related parties. RansomHouse members prefer common sense, good conflict management and intelligent negotiations in an effort to achieve fulfillment of each party's obligations instead of having non-constructive arguments. These are necessary and sufficient principles that lead to amicable agreements and sometimes even to subsequent productive and friendly cooperation.
RansomHouse shares the opinion of both Red and Blue teams regarding the threats of data leaks. The very possibility of such incidents taking place is a strong incentive to make the private sector, corporations and the public aware of data security and privacy issues and should make those involved in 3rd parties' personal information collection and storage responsible and respectful of their responsibilities. Unfortunately, more often than not CEOs prefer to close their eyes on cybersecurity saving budget on their staff or spending huge amounts of money mindlessly, which inevitably leads to vulnerabilities.
We believe that the culprits are not the ones who found the vulnerability or carried out the hack, but those who did not take proper care of security. The culprits are those who did not put a lock on the door leaving it wide open inviting everyone in. People are inherently curious and are eager to learn the object of their interest. Usually corporations respond to the message that their "doors are wide open" in negative context, direct threats or silence. In rare cases one could meet gratitude and ridiculously small payments that do not cover even 5% of an enthusiast's efforts. Well, the negative reaction is understandable, because the company management will have a hard time explaining millions of dollars spent on security audits and cybersecurity staff high salaries to their shareholders

with some freelancer around pointing out the global mistakes they've made, bringing their managerial skills and the results of spending money to the ground. A close example to you might be Lehman Brothers who were warned about severe vulnerabilities in their economic risk management model six months in advance before the collapse - warned by three enthusiastic economist-mathematicians who got nothing but mocks from the fund.
But evolution cannot be stopped, fitting structures emerge in every environment, and so groups of enthusiasts have emerged on the grounds of data negligence, eager to get paid honestly by streamlining this chaos through public punishment. These methods of making money and pointing out companies' mistakes may be controversial, and when you recall that we are talking about billion-dollar corporations on the opposing side, it becomes clear why the RansomHouse team is so important to engage in dialogue. That is what this project is all about - bringing conflicting parties together, helping them to set up a dialogue and make informed, balanced decisions. The team works hard to find a way out of even the most difficult situations and allow both parties to go forward without changing rules as they go along. Incompetence and fuss is unacceptable when dealing with such cases, which is exactly what happens most often. Here and now we are creating a new culture and streamlining this industry.
Unfortunately, companies that refuse negotiations and reject reasonable arguments, companies that are unwilling to pay for this kind of work - will face reputational and legal costs. In order to highlight these cases we will not only disclose information on our website and official Telegram channel but also attract the attention of journalists, public and third parties to the problem and do everything needed to make the incident as public as possible. Information accessibility is one of the foundations of a civilized society and a way for it to rise above itself and overcome social challenges.
We are strictly against the suffering of any individuals who became victims of other people's irresponsibility and leaks. To the best of our ability we help them by giving an opportunity to make a request through our Official Telegram Channel and have their data package removed from the shared set before it is published. The right to manage personal data is fulfilled here to the extent possible in current circumstances.

Краткий перевод (только слова группы о "себе"):
Наша миссия
©RansomHouse — сообщество профессиональных посредников.
Мы не имеем никакого отношения к взлому, не создаем и не используем программы-вымогатели. Наша основная цель – свести к минимуму ущерб, который может быть нанесен связанным сторонам. Члены RansomHouse предпочитают здравый смысл, хорошее управление конфликтами и разумные переговоры, чтобы добиться выполнения обязательств каждой стороны, а не неконструктивные аргументы. Это необходимые и достаточные принципы, ведущие к мировым соглашениям, а иногда и к последующему продуктивному и дружескому сотрудничеству.
*** К сожалению, чаще всего руководители предпочитают закрывать глаза на кибербезопасность, экономя бюджет на своих сотрудниках или бездумно тратя огромные суммы денег, что неизбежно приводит к уязвимостям.
Мы считаем, что виноваты не те, кто нашел уязвимость или осуществил взлом, а те, кто не позаботился о безопасности должным образом. ***

*** поэтому на почве халатного отношения к данным возникли группы энтузиастов, стремящихся честно получить деньги, упорядочив этот хаос посредством публичного наказания. Эти методы зарабатывания денег и указания на ошибки компаний могут быть спорными, а когда вспоминаешь, что речь идет о корпорациях на миллиарды долларов на противоположной стороне, становится понятно, почему команде RansomHouse так важно вести диалог. Именно для этого и предназначен этот проект – сближение конфликтующих сторон, помощь им в налаживании диалога и принятии взвешенных, взвешенных решений. *** Здесь и сейчас мы создаем новую культуру и оптимизируем эту отрасль.
К сожалению, компании, которые отказываются от переговоров и отвергают разумные доводы, компании, которые не желают платить за такую работу, столкнутся с репутационными и юридическими издержками. Для освещения этих случаев мы будем не только раскрывать информацию на нашем сайте и официальном Telegram-канале, но и привлекать внимание журналистов, общественности и третьих лиц к проблеме и делать все необходимое, чтобы инцидент был максимально публичным. ***
Мы категорически против страданий любых лиц, ставших жертвами чужой безответственности и утечек. ***

Страница "Rules"

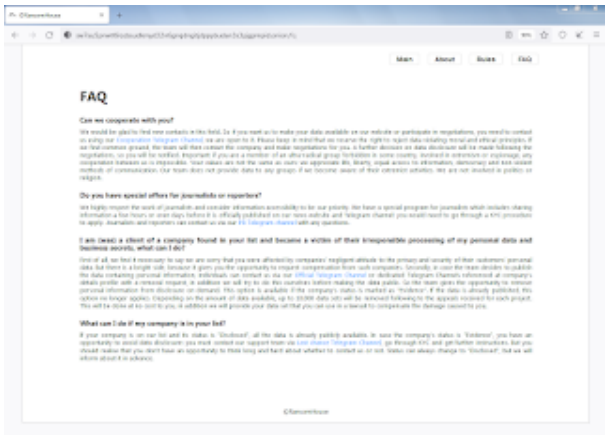


Содержание:
Terms of service
1. Payment
1.1. A Bitcoin wallet will be provided to the customer directly in the chat room when the customer is ready to pay;
1.2. One bitcoin must be transferred to payment wallet for verification first; the remaining amount must be transferred after confirming the transaction from our side;
2. Participation of third-parties
2.1. Participation of police departments is prohibited;
2.2. Participation of FBI, CIA, NSA or other special agencies is prohibited;
2.3. Participation of third-party negotiators is prohibited;
2.4. Violation of clauses 2.1.-2.3. of "Terms of service" causes immediate termination of negotiations and all reached agreements. In this case all the data the team has will be disclosed on the website, Telegram channel and sent to all involved companies and individuals.

3. Post-transaction guarantees
3.1. All uploaded information will be removed from the team's servers;
3.2. All posts/websites/pages etc. posted by the team and associated with the data leak will be removed;
3.3. All backdoors exploited by the team will be removed;
3.4. Personal data will not be shared with third parties by the team;
3.5. A list of information security recommendations will be provided to the head of the company;
3.6. Decryption software, guidance and support will be provided if required;
3.7. Current vulnerabilities will never be used by the team for further attacks. In case new vulnerabilities will be discovered, the company will be notified.

Краткий перевод:
Условия обслуживания
1. Оплата
1.1. Биткойн-кошелек будет дан клиенту прямо в чате, когда клиент будет готов заплатить;
1.2. Сначала надо перевести 1 биткойн на кошелек для проверки; оставшуюся сумму нужно перевести после подтверждения транзакции с нашей стороны;
2. Участие третьих лиц
2.1. Участие отделений полиции запрещено;
2.2. Участие ФБР, ЦРУ, АНБ или других спец. агентств запрещено;
2.3. Участие сторонних переговорщиков запрещено;
2.4. Нарушение пунктов 2.1.-2.3. "Условий обслуживания" влечет за собой немедленное прекращение переговоров и всех достигнутых договоренностей. В этом случае все данные, которые есть у команды, будут раскрыты на сайте, в Telegram-канале и отправлены всем заинтересованным компаниям и частным лицам.
3. Гарантии после сделки
3.1. Вся загруженная информация будет удалена с серверов команды;
3.2. Все сообщения/веб-сайты/страницы и пр., размещенные командой и связанные с утечкой данных, будут удалены;
3.3. Все бэкдоры, используемые командой, будут удалены;
3.4. Персональные данные не будут переданы командой третьим лицам;
3.5. Список рекомендаций по информационной безопасности будет предоставлен руководителю компании;
3.6. При необходимости будет предоставлена программа для расшифровки, руководство и поддержка;
3.7. Текущие уязвимости никогда не будут использованы командой для дальнейших атак. При обнаружениия новых уязвимостей компания будет уведомлена об этом.---

Страница "FAQ"



Содержание:

FAQ

Can we cooperate with you?

We would be glad to find new contacts in this field. So if you want us to make your data available on our website or participate in negotiations, you need to contact us using our Cooperation Telegram Channel, we are open to it. Please keep in mind that we reserve the right to reject data violating moral and ethical principles. If we find common ground, the team will then contact the company and make negotiations for you. A further decision on data disclosure will be made following the negotiations, so you will be notified. Important: if you are a member of an ultra-radical group forbidden in some country, involved in extremism or espionage, any cooperation between us is impossible. Your values are not the same as ours: we appreciate life, liberty, equal access to information, democracy and non-violent methods of communication. Our team does not provide data to any groups if we become aware of their extremist activities. We are not involved in politics or religion.

Do you have special offers for journalists or reporters?

We highly respect the work of journalists and consider information accessibility to be our priority. We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.

I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets, what can I do?

First of all, we find it necessary to say we are sorry that you were affected by companies' negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies. Secondly, in case the team decides to publish the data containing personal information, individuals can contact us via our Official Telegram Channel or dedicated Telegram Channels referenced at company's details profile with a removal request, in addition we will try to do this ourselves before making the data public. So the team gives the opportunity to remove personal information from disclosure on demand. This option is available if the company's status is marked as "Evidence". If the data is already published, this option no longer applies. Depending on the amount of data available, up to 10,000 data sets will be removed following to the appeals received for each project. This will be done at no cost to you, in addition we will provide your data set that you can use in a lawsuit to compensate the damage caused to you.

What can I do if my company is in your list?
If your company is on our list and its status is "Disclosed", all the data is already publicly available. In case the company's status is "Evidence", you have an opportunity to avoid data disclosure: you must contact our support team via Last chance Telegram Channel, go through KYC and get further instructions. But you should realise that you don't have an opportunity to think long and hard about whether to contact us or not. Status can always change to "Disclosed", but we will inform about it in advance.
©RansomHouse

Краткий перевод:
ЧЗВ
Можем ли мы сотрудничать с вами?
Мы будем рады новым контактам в этой области. Поэтому, если вы хотите, чтобы мы сделали ваши данные доступными на нашем сайте или участвовали в переговорах, вам надо написать нам в наш Telegram-канал... ...мы оставляем за собой право отклонять данные, нарушающие моральные и этические принципы. Если мы найдем точки соприкосновения, команда свяжется с компанией и проведет переговоры. Решение о раскрытии данных будет принято после переговоров... Важно: если вы член запрещенной ...ультрарадикальной группировки, занимающейся экстремизмом или шпионажем, сотрудничество между нами невозможно. Ваши ценности отличаются от наших: мы ценим жизнь, свободу, равный доступ к информации, демократию и ненасильственные методы общения. Наша команда не предоставляет данные каким-либо группам, если нам становится известно об их экстремистской деятельности. Мы не занимаемся политикой или религией.
Есть ли у вас специальные предложения для журналистов или репортеров?
Мы очень уважаем труд журналистов и считаем доступность информации нашим приоритетом. У нас есть специальная программа для журналистов, которая включает в себя обмен информацией за несколько часов или даже дней до ее официальной публикации на нашем новостном сайте и в Telegram-канале: для подачи заявки вам необходимо пройти процедуру KYC. Журналисты и репортеры могут связаться с нами через наш PR Telegram-канал...
Я являюсь (был) клиентом компании из вашего списка и стал жертвой их безответственной обработки моих личных данных и коммерческой тайны, что я могу сделать?
Прежде всего... сожалеем о том, что вы пострадали от небрежного отношения компаний к конфиденциальности и безопасности персональных данных своих клиентов. Но ...это дает вам возможность требовать компенсацию... ...если команда решит опубликовать данные, содержащие личную информацию, люди могут связаться с нами через наш официальный канал Telegram или специальные каналы Telegram, указанные в профиле компании, с запросом на удаление... ...Эта опция доступна, если статус компании отмечен как «Доказательства». Если данные уже опубликованы, этот параметр больше не применяется... Это будет сделано бесплатно для вас, кроме того, мы предоставим ваш набор данных, который вы сможете использовать в судебном процессе для возмещения причиненного вам ущерба.
Что мне делать, если моя компания есть в вашем списке?
Если ваша компания есть в нашем списке и у нее статус «Раскрыта», то все данные уже находятся в открытом доступе. В случае статуса компании «Доказательство» у вас есть

возможность избежать разглашения данных: вам надо связаться с нашей службой поддержки через Telegram-канал «Последний шанс», пройти KYC и получить дальнейшие инструкции. Но вы должны понимать, что у вас нет возможности долго и упорно думать, обращаться к нам или нет. Статус всегда может измениться на "Раскрыт", но мы сообщим об этом заранее. ©RansomHouse

Внимание! Различия с первым вариантом могут быть опубликованы в разделе для обновлений, после основной статьи.

Технические детали + IOC

Используемое вредоносное ПО 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 типов файлов, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

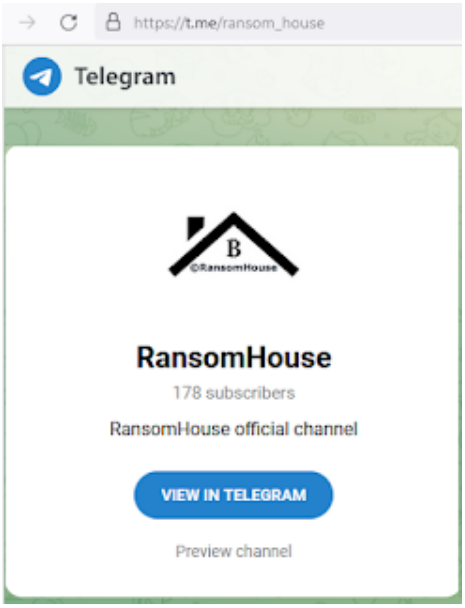
Файлы, связанные с этим Ransomware:
<ransom_note>.txt - название файла индивидуальной записки;
<random>.exe - условное название вредоносного файла.

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

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Telegram: ransom_house
Tor-URL: hxxx://xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion
Email: -
BTC: -



Результаты анализов:
IOC: VT, HA, IA, TG, AR, VMR, JSB

MD5: -

Степень распространённости: низкая.
Информация дополняется. 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 ===

Read to links:

Message + Message + **myMessage**
Write-up, Topic of Support
*

Thanks:

RakeshKrish12
Andrew Ivanov (article author)
***
to the victims who sent the samples

Pipikaki

Pipikaki Ransomware

Pipikaki Doxware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные бизнес-пользователей с помощью комбинации алгоритмов AES+RSA, а затем требует написать вымогателям в Skype, ICQ или на email, чтобы вернуть файлы. Оригинальное название: Pipikaki. На файле написано: нет данных.

Обнаружения:

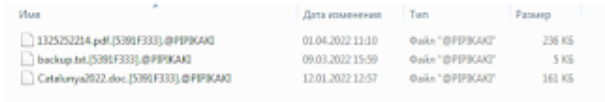
DrWeb ->
BitDefender ->
ESET-NOD32 ->
Kaspersky ->
Malwarebytes ->
Microsoft ->
Rising ->
Tencent ->
TrendMicro ->

© Генеалогия: ??? >> Pipikaki

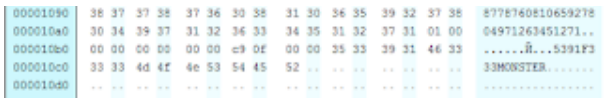
Сайт "ID Ransomware" это пока не идентифицирует.
Информация для идентификации

Активность этого крипто-вымогателя была в конце апреля 2022 г. Ориентирован на англоязычных пользователей, может распространяться по всему миру.

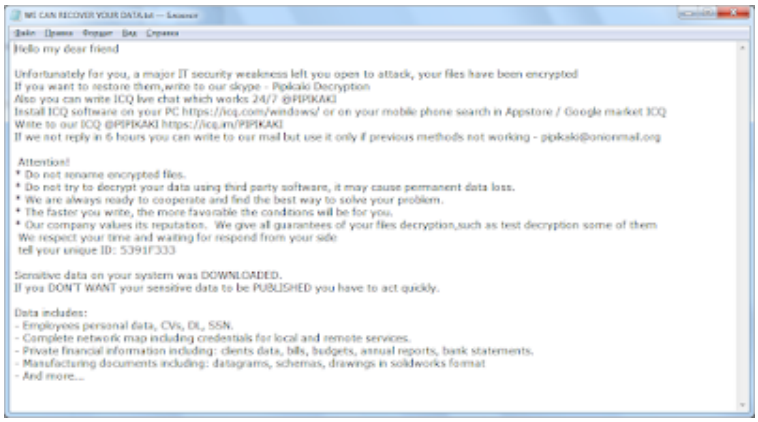
К зашифрованным файлам добавляется расширение: **.[5391F333].@PIPIKAKI**



В конец кода зашифрованного файла добавляется маркер **5391F333MONSTER**



Записка с требованием выкупа называется: **WE CAN RECOVER YOUR DATA.txt**



Содержание записки о выкупе:
Hello my dear friend
Unfortunately for you, a major IT security weakness left you open to attack, your files have been encrypted
If you want to restore them,write to our skype - Pipikaki Decryption
Also you can write ICQ live chat which works 24/7 @PIPIKAKI
Install ICQ software on your PC https://icq.com/windows/ or on your mobile phone search in Appstore / Google market ICQ
Write to our ICQ @PIPIKAKI https://icq.im/PIPIKAKI
If we not reply in 6 hours you can write to our mail but use it only if previous methods not working - pipikaki@onionmail.org
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* We are always ready to cooperate and find the best way to solve your problem.
* The faster you write, the more favorable the conditions will be for you.
* Our company values its reputation. We give all guarantees of your files decryption,such as test decryption some of them
We respect your time and waiting for respond from your side
tell your unique ID: 5391F333
Sensitive data on your system was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.
Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Перевод записки на русский язык:
Привет, мой дорогой друг
К сожалению для вас, из-за серьезной уязвимости в ИТ-безопасности вы оказались уязвимы для атак, ваши файлы зашифрованы.

Если хотите их восстановить, пишите в наш скайп - Pipikaki Decryption
Также вы можете написать в онлайн-чат ICQ, который работает 24/7 @PIPIKAKI.
Установите программу ICQ на свой ПК https://icq.com/windows/ или на мобильный телефон ищите в Appstore/Google market ICQ
Пишите в наш ICQ @PIPIKAKI https://icq.im/PIPIKAKI
Если мы не ответим в течение 6 часов, вы можете написать на нашу почту, но использовать ее, только если предыдущие способы не работают - pipikaki@onionmail.org
Внимание!
* Не переименовывайте зашифрованные файлы.
* Не пытайтесь расшифровать свои данные с помощью сторонних программ, это может привести к безвозвратной потере данных.
* Мы всегда готовы к сотрудничеству и найдем лучший способ решить вашу проблему.
* Чем быстрее вы напишете, тем выгоднее будут для вас условия.
* Наша компания дорожит своей репутацией. Мы даем все гарантии расшифровки ваших файлов, в том числе тестовую расшифровку некоторых из них
Мы уважаем ваше время и ждем ответа с вашей стороны
сообщите свой уникальный ID: 5391F333
Конфиденциальные данные из вашей системе были СКАЧАНЫ.
Если вы НЕ ХОТИТЕ, чтобы ваши конфиденциальные данные были ОПУБЛИКОВАНЫ, вы должны действовать быстро.
Данные включают:
- Персональные данные сотрудников, CV, DL, SSN.
- Полная карта сети, включая учетные данные для локальных и удаленных служб.
- Частная финансовая информация, включая: данные клиентов, счета, бюджеты, годовые отчеты, банковские выписки.
- Производственная документация, в том числе: дейтаграммы, схемы, чертежи в формате SolidWorks
- И более...

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

Технические детали + IOC

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 типов файлов, 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:
WE CAN RECOVER YOUR DATA.txt - название файла с требованием выкупа;
<random>.exe - случайное название вредоносного файла

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

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

Мьютексы:
См. ниже результаты анализов.

Сетевые подключения и связи:
Skype: Pipikaki Decryption
ICQ: @PIPIKAKI
Email: pipikaki@onionmail.org

См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:
IOC: VT, HA, IA, TG, AR, VMR, JSB

MD5: -

Степень распространённости: низкая.
Информация дополняется. 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 ===

Read to links:

myMessage + Message + Message
Write-up, Topic of Support, **Topic of Support**
*

Thanks:

Andrew Ivanov (article author)
***
***
to the victims who sent the samples