DarkSide

DarkSide Ransomware

DarkSide Hand-Ransomware

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

Этот крипто-вымогатель шифрует данные бизнес-пользователей и предприятий с помощью Salsa20+RSA-1024, а затем требует выкуп в несколько миллионов долларов в BTC, чтобы вернуть файлы. Оригинальное название: DarkSide. Написан на Python.

Обнаружения:
DrWeb -> Trojan.Encoder.32305, Trojan.Encoder.32386, Trojan.Encoder.33337
BitDefender -> Gen:Variant.Razy.734971
Avira (no cloud) -> TR/Crypt.XPACK.Gen
ESET-NOD32 -> A Variant Of Generik.MMUYADA
Kaspersky -> Trojan-Ransom.Win32.Gen.xyl
Malwarebytes -> Ransom.DarkSide
Rising -> Ransom.Gen!8.DE83 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Trojan.Crypt.Edxi
TrendMicro -> TROJ_GEN.R002H09H820, Ransom.Win32.DARKSIDE.THHABBOA

© Генеалогия: Sodinokibi / REvil ? => DarkSide > BlackMatter

Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.<random>**

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

Началом распространения можно считать появление на форумах кибер-андеграунда в начале августа 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **README.<random>.TXT**

Пример записки от вымогателей: README.97866000.TXT

Содержание записки о выкупе:

```
----------- [ Welcome to Dark ] ------------->
What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot
decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will
restore all your network.
Follow our instructions below and you will recover all your data.
Data leak
---------------------------------------------
First of all we have uploaded more then 100 GB data.
Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
 - Quality data
 - And more other...
Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/***
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.
What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our
interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case
of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.
How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/***
When you open our website, put the following data in the input form:
Key:
*** [всего 567 знаков]
!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

Перевод записки на русский язык:

---------- [Добро пожаловать в Dark] ------------>

Что случилось?

Ваши компьютеры и серверы зашифрованы, резервные копии удалены. Мы используем надежные алгоритмы шифрования, поэтому вы не сможете расшифровать свои данные.

Но вы можете все восстановить, купив у нас специальную программу - универсальный дешифратор. Эта программа восстановит всю вашу сеть.

Следуйте нашим инструкциям ниже и вы восстановите все свои данные.

Утечка данных

Во-первых, мы загрузили более 100 ГБ данных.

Пример данных:

- Данные бухгалтерского учета
- Исполнительные данные
- Данные о продажах
- Данные службы поддержки
- Маркетинговые данные
- Данные о качестве
- И многое другое ...

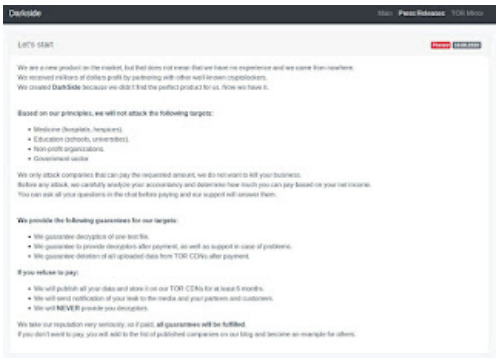
Ваша личная страница утечки: http://darksidedxcftmqa.onion/blog/article/id/***
Данные предварительно загружены и будут автоматически опубликованы, если вы не заплатите.
После публикации ваши данные будут доступны не менее 6 месяцев на наших серверах tor cdn.
Мы готовы:
- Чтобы предоставить вам доказательства украденных данных
- Чтобы предоставить вам универсальный инструмент для дешифрования всех зашифрованных файлов.
- Удалить все украденные данные.
Какие гарантии?

Мы дорожим своей репутацией. Если мы не будем выполнять свою работу и обязательства, нам никто не будет платить. Это не в наших интересах.
Все наши программы для дешифрования отлично протестированы и расшифруют ваши данные. Мы также окажем поддержку при возникновения проблем.
Мы гарантируем бесплатную расшифровку одного файла. Зайдите на сайт и свяжитесь с нами.
Как получить доступ на сайт?

Используя браузер TOR:
1) Загрузите и установите браузер TOR с этого сайта: https://torproject.org/
2) Откройте наш сайт: http://darksidfqzcuhtk2.onion/***
Когда вы открываете наш веб-сайт, введите в форму ввода следующие данные:
Ключ:
*** [всего 567 знаков]
!!! ОПАСНОСТЬ !!!
НЕ ИЗМЕНЯЙТЕ и НЕ ПЫТАЙТЕСЬ ВОССТАНОВИТЬ файлы самостоятельно. Мы НЕ сможем их ВОССТАНОВИТЬ.
!!! ОПАСНОСТЬ !!!

Технические детали

Распространяется как RaaS на форумах кибер-андеграунда. Использует сеть Tor для сайта и публикации там же украденной информации компаний-жертв.



Текст со скриншота:
Darkside
Let's start
We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created DarkSide because we didn't find the perfect product for us. Now we have it
Based on our principles, we will not attack the following targets:
• Medicine (hospitals, hospices).
• Education (schools, universities).
• Non-profit organizations.

• Government sector.
We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.
We provide the following guarantees for our targets:
• We guarantee decryption of one test file.
• We guarantee to provide decryptors after payment, as well as support in case of problems.
• We guarantee deletion of all uploaded data from TOR CDNs after payment.
If you refuse to pay:
• We will publish all your data and store it on our TOR CDNs for at least 6 months.
• We will send notification of your leak to the media and your partners and customers.
• We will NEVER provide you decryptors.
We take our reputation very seriously, so if paid, all guarantees will be fulfilled.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

Перевод на русский язык:
Darkside
Давайте начнем
Мы новый продукт на рынке, но это не значит, что у нас нет опыта и мы пришли из ниоткуда.
Мы получили прибыль в миллионы долларов, сотрудничая с другими известными крипто-локерами.
Мы создали DarkSide, потому что не нашли для себя идеального продукта. Теперь у нас он есть
Исходя из наших принципов, мы не будем атаковать следующие цели:
• Медицина (больницы, хосписы).
• Образование (школы, университеты).
• Некоммерческие организации.
• Государственный сектор.
Мы атакуем только компании, которые могут заплатить запрошенную сумму, мы не хотим губить ваш бизнес.
Перед любой атакой мы тщательно анализируем вашу бухгалтерию и определяем, сколько вы можете заплатить, исходя из вашего чистого дохода.
Вы можете задать все интересующие вас вопросы в чате перед оплатой, и наша служба поддержки ответит на них.
Мы предоставляем следующие гарантии для наших целей:
• Мы гарантируем расшифровку одного тестового файла.
• Мы гарантируем предоставление дешифраторов после оплаты, а также поддержку в случае возникновения проблем.
• Мы гарантируем удаление всех загруженных данных из TOR CDN после оплаты.
Если вы отказываетесь платить:
• Мы опубликуем все ваши данные и будем хранить их на наших TOR CDN в течение как минимум 6 месяцев.
• Мы отправим уведомление о вашей утечке средствам массовой информации, вашим партнерам и клиентам.
• Мы НИКОГДА не предоставим вам дешифраторы.
Мы очень серьезно относимся к своей репутации, поэтому в случае оплаты все гарантии будут выполнены.
Если вы не хотите платить, вы добавитесь в список опубликованных компаний в нашем блоге и станете примером для других.

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 пару методов для проверки принадлежности ПК к некоторым странам СНГ (проверяет GetSystemDefaultUILanguage - язык системы, GetUserDefaultLangID - язык пользователя по умолчанию). Таким образом, не должен шифровать файлы из этих стран.

➤ **Перед шифрованием завершает следующие процессы**, которые могут помешать шифрованию файлов:
sql
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
winword
wordpad
notepad

Список файловых расширений, подвергающихся шифрованию:
Все файлы, кроме тех, что находятся в списках пропускаемых расширений, файлов, папок, процессов.
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, .deskthemepack, .diagcab, .diagcfg, .diagpkg, .dll, .drv, .exe, .hlp, .hta, .icl, .icns, .ico, .ics, .idx, .key, .ldf, .lnk, .lock, .mod, .mpa, .msc, .msi, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .pdb, .prf, .ps1., .rom, rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx (50 расширений).

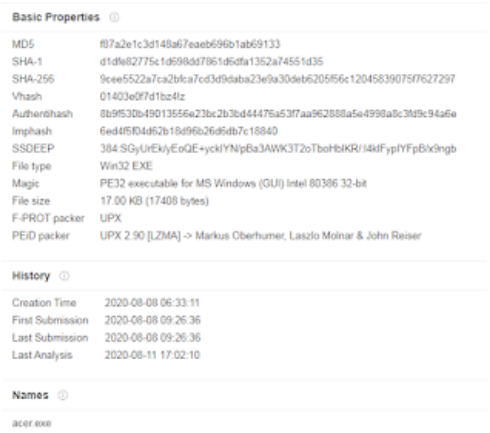
Список пропускаемых директорий:
windows
appdata
application data
boot
google
mozilla
program files

program files (x86)
programdata
system volume information
tor browser
windows.old
intel
msocache
perflogs
x64dbg
public
all users
default

Список пропускаемых файлов:
$recycle.bin
config.msi
$windows.~bt
$windows.~ws

Список пропускаемых процессов:
vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe

Файлы, связанные с этим Ransomware:
acer.exe - исполняемый файл
README.<random>.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:
Мьютекс Global\\3e93e49583d6401ba148cd68d1f84af7 создается, чтобы могла работать только одна копия Ransomware.

См. ниже результаты анализов.

Сетевые подключения и связи:
Tor-URL: xxxx://darksidedxcftmqa.onion/
Email: -
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

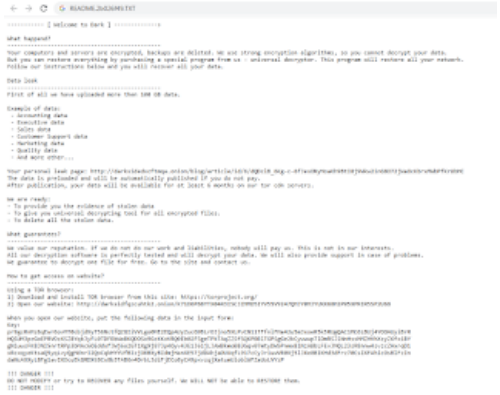
Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Вариант от 11 августа 2020:
Пост в Твиттере >>
Расширение: **.2b026f49**
Записка: README.2b026f49.TXT
Результаты анализов: **VT** + **HA**



➤ Содержание записки от вымогателей:
---------- [Welcome to Dark] ---------->
What happend?

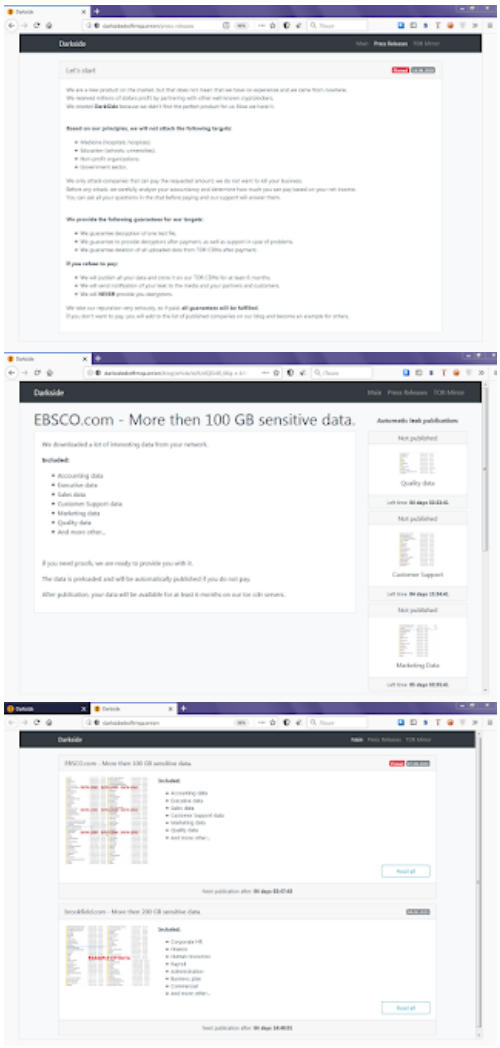
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.
Data leak

First of all we have uploaded more then 100 GB data.
Example of data:
- Accounting data
- Executive data
- Sales data
- Customer Support data
- Marketing data
- Quality data
- And more other...
Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9BtI8j9Wkw2inG8O72jWaOcKbrxMWbPfKrUbHC
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.
What guarantees?

We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.
How to get access on website?

Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website:
http://darksidfqzcuhtk2.onion/K71D6P88YTX04R3ISCJZHMD5IYV55V9247QHJY0HJYUXX68H2P05XPRIR5SP2U68
When you open our website, put the following data in the input form:
Key:
pr9gzRnMz6qEwr6ovMT0cbjd9yT56NctfQZGIiVVL [всего 567 знаков]
!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!

➤ Ссылки на сообщение для пострадавшего:
http://darksidedxcftmqa.onion/blog/article/id/6
http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9BtI8j9Wkw2inG8O72jWaOcKbrxMWbPfKrUbHC

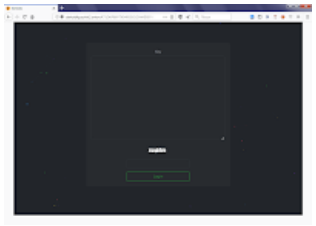


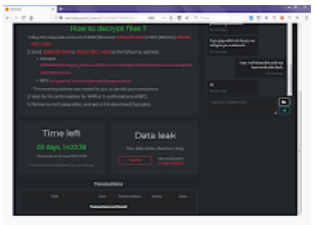
➤ Сообщение для пострадавшей компании:
EBSCO.com - More then 100 GB sensitive data.
Automatic leak publication:
We downloaded a lot of interesting data from your network.
Included:

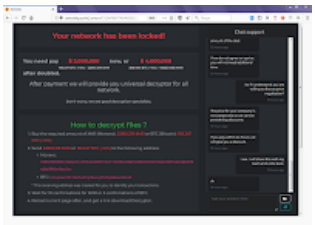
- Accounting data
- Executive data
- Sales data
- Customer Support data
- Marketing data
- Quality data
- And more other...

if you need proofs, we are ready to provide you with it.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

➤ Сообщение для пострадавшей компании до и после ввода ключа:

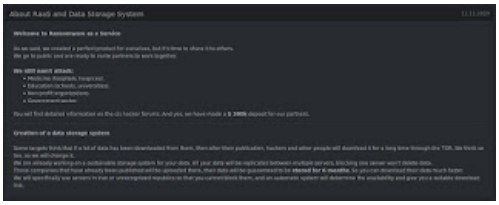






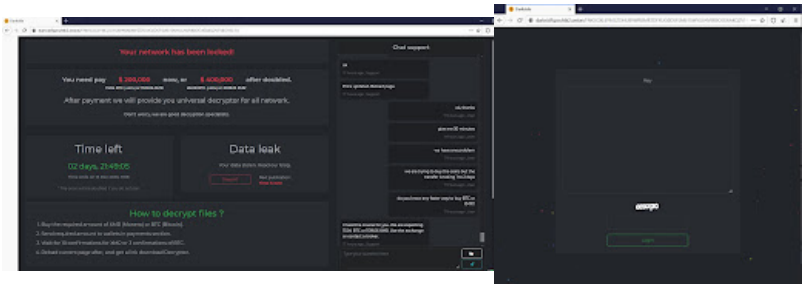
Сумма выкупа: $ 2,000,000 / 193.247 BTC / 22810.219 XMR
Monero-кошелек:
86R5YKD3DbMTJ1mgqiYjjsVULxwcxN5h5YyJt7Sz4B2oZEpZCnGBDZY4DG293xeeZSeF6iaDJqAoRVMeQXgUNM5x3fzyZru
BTC-кошелек: bc1qena2vfl7xhc5ad7q06eeuyd563ykxmwardnt2d

Вариант от 26 августа 2020:
Пост в Твиттере >>
Расширение (пример): **.97866079**
Сообщение >>



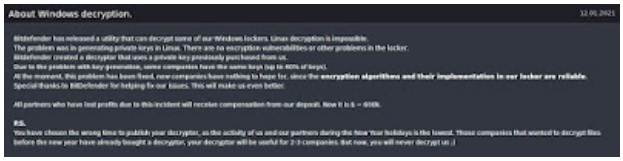
Обновление от 13 ноября 2020:
Статья на сайте BleepingComputer >>
Программа-вымогатель DarkSide создает в Иране базу для хранения украденной информации.
DarkSide Ransomware работает как RaaS, где разработчики отвечают за программирование ПО Ransomware и сайта платежей, а аффилированные лица нанимаются для взлома предприятий и шифрования их устройств. Разработчики забирают 10-25%, а аффилированные лица получают 75-90% от любых произведенных ими выкупных платежей. Чтобы пресечь вымогательство правоохранительные органы и компании, занимающиеся кибербезопасностью, активно пытаются заблокировать сайты утечки данных. Вопреки этому DarkSide заявляет, что они планируют создать распределенную "устойчивую систему хранения" в Иране для хранения украденных данных жертвы в течение шести месяцев.
Представитель DarkSide заявляет, что не разрешает атаки на:
 - медицинские учреждения (больницы, хосписы);
- образовательные учреждения (школы, университеты);
- некоммерческие организации;
- государственный сектор.
Но сдержит ли DarkSide свое обещание не нацеливаться на них, покажет время.

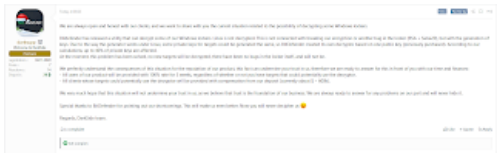
Обновление от 10 декабря 2020:
Сообщение >>
Tor-URL: xxxx://darksidfqzcuhtk2.onion



Обновление от 11 января 2021:
Специалисты BitDefender выпустили дешифровщик для файлов, зашифрованных DarkSide Ransomware.

Обновление от 12 января 2021:
Сообщение >>
Сообщение >>
Вымогатели внесли изменения в шифрование и сообщили об этом на форуме.

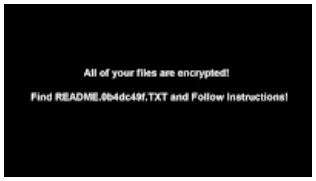


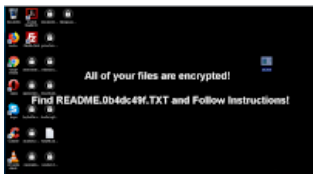


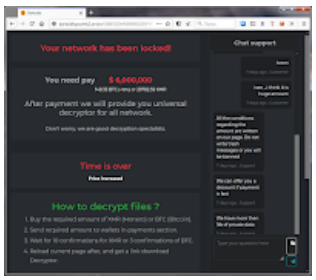
Вариант от 15 января 2921:
Сообщение >>
Расширение (пример): **.c06622a1**
Записка (пример): README.c06622a1.TXT
Штамп даты: 23 декабря 2020.
Результат анализов: **VT + VMR**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33337
ESET-NOD32 -> A Variant Of Win32/Filecoder.DarkSide.A
TrendMicro -> Ransom.Win32.DARKSIDE.SMYAAK-B
Вариант от 24 января 2021:
Сообщение >>
Расширение: **.c06622a1**
Tor-URL: darksidedxcftmqa.onion/***
Tor-URL: darksidfqzcuhtk2.onion/***
URL: securebestapp20.com

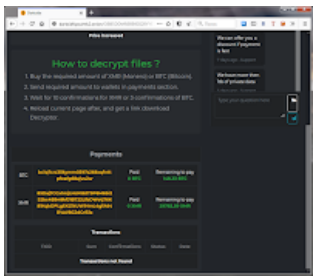
Вариант от 3 февраля 2021:
Расширение: **.0b4dc49f**
Примеры записок:
README.418990b0.TXT
README.0b4dc49f.TXT
Результы анализов: **VT + AR + IA**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33337
ALYac -> Trojan.Ransom.DarkSide
BitDefender -> Gen:Heur.Ransom.RTH.1
ESET-NOD32 -> A Variant Of Win32/Filecoder.DarkSide.A

Malwarebytes -> Ransom.DarkSide
Symantec -> Ransom.Darkside
TrendMicro -> Ransom.Win32.DARKSIDE.SMYAAK-B

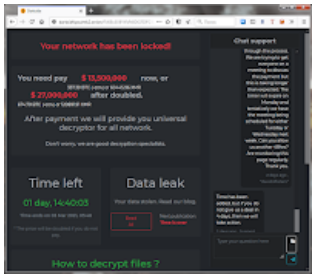


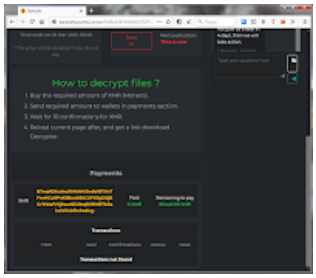




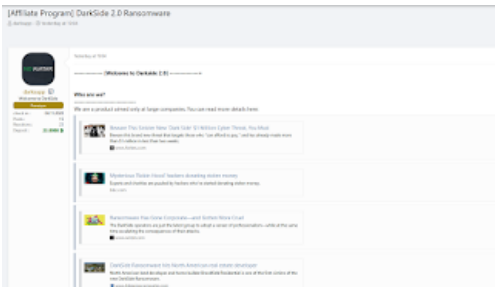


Вариант 28 февраля 2021:
Сообщение >>
Файл: calimalimodumator.exe
Результаты анализов: **AR** + **AR** + **VT** + **HA**
Вариант 28 февраля 2021:
Сообщение >>
Расширение: .0b4dc49f
Записка: README.0b4dc49f.TXT
URL: xxxx://darksidfqzcuhtk2.onion/***
Файл: homie.exe, MicSwitch.exe
Результаты анализов: **AR** + **VT** + **IA**





Обновление от 11 марта 2021:
Сообщение >>

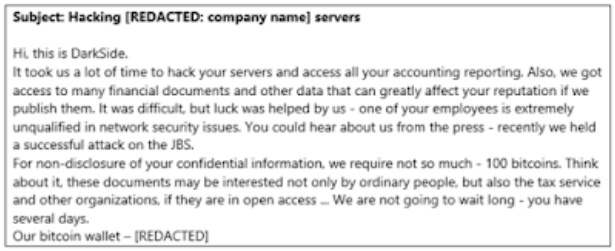


Вариант от 1 мая 2021:
Сообщение >>
Расширение: .425b93ba
Записка: README.425b93ba.TXT

Tor-URL: hxxx://dark24zz36xm4y2phwe7yvnkkkkhxionhfrwp67awpb3r3bdcneivoqd.onion/*
Результаты анализов: **VT + AR**
➤ Обнаружения:
DrWeb -> Trojan.Encoder.33763
BitDefender -> Trojan.GenericKD.46189032
ESET-NOD32 -> A Variant Of Win32/Filecoder.DarkSide.B
Malwarebytes -> Ransom.DarkSide
Microsoft -> Ransom:Win32/DarkSide.DA!MTB
TrendMicro -> Ransom_DarkSide.R002C0DE121

Сообщение от 18 мая 2021:
Статья на сайте BleepingComputer >>
Вымогатели, использующие DarkSide Ransomware, собрали с пострадавших около 90 миллионов долларов в виде выкупа, выплаченного жертвами за последние девять месяцев на несколько BTC-кошельков. Подсчитано, что разработчики DarkSide Ransomware получил из общей прибыли биткойны на сумму 15,5 млн долларов. Филиалы или партнеры обычно получают львиную долю денег, потому что они делают большую часть работы: взламывают сети жертв, крадут данные и развертывают вредоносное ПО для шифрования файлов. В случае с DarkSide они получали от 75% до 90% прибыли, в зависимости от размера выкупа.

Сообщение от 18 июня 2021:
Элементы вымогательства (email-адреса, BTC-кошелек) будут идентифицироваться на сайте "ID Ransomware" как "Fake DarkSide".
Статья TrendMocro >>
Статья BpeepingComputer >>
От имени DarkSide с 4 июня 2021 года проводится мошенническая email-компания, нацеленная на email-адреса компаний энергетической и пищевой промышленности. Никаких фактических атак не было прослежено.
Целевые станы: Аргентина, Австралия, Канада, США, Великобритания, Индия, Китай, Колумбия, Мексика, Нидерланды, Таиланд,
Email: darkside@99email.xyz, darkside@solpatu.space
BTC: bc1qcwrl3yaj8pqevj5hw3363tycx2x6m4nkaaqd5e
Сумма выкупа до 100 BTC.


Subject: Hacking [REDACTED: company name] servers

Hi, this is DarkSide.
It took us a lot of time to hack your servers and access all your accounting reporting. Also, we got access to many financial documents and other data that can greatly affect your reputation if we publish them. It was difficult, but luck was helped by us - one of your employees is extremely unqualified in network security issues. You could hear about us from the press - recently we held a successful attack on the JBS.
For non-disclosure of your confidential information, we require not so much - 100 bitcoins. Think about it, these documents may be interested not only by ordinary people, but also the tax service and other organizations, if they are in open access ... We are not going to wait long - you have several days.
Our bitcoin wallet – [REDACTED]

➤ Образец текста электронного письма:
Hi, this is DarkSide.
It took us a lot of time to hack your servers and access all your accounting reporting. Also, we got access to many financial documents and other data that can greatly affect your reputation if we publish them.
It was difficult, but luck was helped by us - one of your employees is extremely unqualified in network security issues. You could hear about us from the press - recently we held a successful attack on the Colonial Pipeline.

For non-disclosure of your confidential information, we require not so much - 100 bitcoins. Think about it, these documents may be interested not only by ordinary people, but also the tax service and other organizations, if they are in open access ... We are not going to wait long - you have several days.
Our bitcoin wallet - bc1qcwrl3yaj8pqevj5hw3363tycx2x6m4nkaaqd5e
---
Биткойн-кошелек в конце каждого письма одинаков для всех целей. На момент написания этого сообщения на BTC-кошелёк платежи не поступали.
Кроме рассылки целевых email-писем те же злоумышленники заполнили контактные формы на сайтах некоторых компаний. Содержание такое же, как и в email-письмах. Один IP-адрес отправителей, 205.185.127.35, оказался выходным узлом сети Tor.

«В целом, эта кампания выглядит дилетантской по сравнению с известными предыдущими мероприятиями DarkSide. Мы считаем, что большинство компаний не будут платить эту сумму, пока не получат какие-либо реальные доказательства того, что сеть была скомпрометирована и конфиденциальные могут быть опубликованы», - сообщает Trend Micro.

***
Итак, **проект DarkSide закрыт**, а на его основе был запущен другой вымогательский проект, который называется **BlackMatter Ransomware**. Исследователи считают его прямым продолжением DarkSide, но так ли на самом деле, никто не знает.

Ссылка на отдельную статью в Даджесте >>

Статья на сайте BleepingComputer >>

Исследования прекращены. Статья закрыта.

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

Внимание!
Файлы можно расшифровать!
Скачайте DarkSide Decryptor по ссылке >>
Прочтите инструкцию на сайте BitDefender.

Added later:

Write-up by Bleeping Computer (on August 21, 2020)
Darkside Ransomware Decryption Tool (on January 11, 2021)
Write-up by Bleeping Computer (on January 11, 2021)

Thanks:

MalwareHunterTeam, Ravi, Michael Gillespie
Andrew Ivanov (author)
Vitali Kremez, Lawrence Abrams,
to the victims who sent the samples