

# AnteFrigus

---

 [id-ransomware.blogspot.com/2019/11/antefrigus-ransomware.html](http://id-ransomware.blogspot.com/2019/11/antefrigus-ransomware.html)



## AnteFrigus Ransomware

---

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

---

Этот крипто-вымогатель шифрует данные пользователей с помощью AES, а затем требует выкуп в \$1.995, который увеличивается через 4 дня до \$3.990. Оригинальное название: AnteFrigus. На файле написано: нет данных.

### Обнаружения:

**DrWeb** -> Trojan.PWS.Siggen2.38675, Trojan.Encoder.30119

**BitDefender** -> Trojan.GenericKD.32711050

**ALYac** -> Trojan.Ransom.AnteFrigus

**Avira (no cloud)** -> TR/Crypt.Agent.yyhfq

**ESET-NOD32** -> A Variant Of Win32/Kryptik.GYHS

**Kaspersky** -> Trojan.Win32.Zenpak.rbj

**Malwarebytes** -> Trojan.MalPack.GS

© Генеалогия: AnteFrigus > Prometey



Изображение — логотип статьи

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





[+] Что случилось? [+]

Ваши файлы зашифрованы и сейчас недоступны. Вы можете проверить это: все файлы на вашем компьютере имеют расширение hssjyh.

Кстати, все можно восстановить (вернуть), но вы должны следовать нашим инструкциям. В противном случае вы не можете вернуть свои данные (НИКОГДА).

[+] Какие гарантии? [+]

Это просто бизнес. Мы абсолютно не заботимся о вас и ваших сделках, кроме получения выгоды. Если мы не выполняем свою работу и обязательства - никто не будет сотрудничать с нами. Это не в наших интересах.

Чтобы проверить возможность возврата файлов, вы должны зайти на наш сайт. Там вы можете бесплатно расшифровать один файл. Это наша гарантия.

Если вы не будете сотрудничать с нашим сервисом - для нас это не имеет значения. Но вы потеряете свое время и данные, ведь только у нас есть закрытый ключ. На практике время гораздо ценнее денег.

[+] Как получить доступ на сайт? [+]

У вас есть два пути:

1) [Рекомендуется] Использовать браузер TOR!

а) Загрузите и установите браузер TOR с этого сайта: <https://torproject.org/>

б) Откройте наш веб-сайт:

<http://yboa7nidpv5jdtumgfm4fmmvju3ccxlleut2xvzgn5uqlbjd5n7p3kid.onion/?hssjyh>

(Если вы не можете перейти по ссылке или по другим причинам, напишите на электронную почту технической поддержки: [antefrigus@cock.li](mailto:antefrigus@cock.li))

2) Если TOR заблокирован в вашей стране, попробуйте использовать VPN! За это:

а) Откройте любой браузер (Chrome, Firefox, Opera, IE, Edge), загрузите и установите бесплатную программу VPN и загрузите браузер TOR с этого сайта <https://torproject.org/>

б) Если у вас возникли трудности с покупкой биткойнов или вы сомневаетесь в покупке расшифровщика, обратитесь в любую компанию по восстановлению данных в вашей стране, которая предоставит вам больше гарантий и возьмет на себя процедуру покупки и расшифровки. Почти все такие компании слышали о нас и знают, что наша программа расшифровки работает, поэтому они могут вам помочь.

Когда вы открываете наш сайт, введите следующие данные в форму ввода:

Ключ:Pjg/ODo4PD08PD87OTg5Nyhoa3RwdShvenpxgG8oSKEOTw8Njk4OidOaUM2aXIFJw==

Название расширения:

hssjyh-----

!!!ОПАСНОСТЬ !!!

НЕ пытайтесь изменить файлы самостоятельно, НЕ используйте любую стороннюю программу для восстановления ваших данных или антивирусные решения - это может повлечь за собой повреждение личного ключа и, как результат, потерю всех данных.

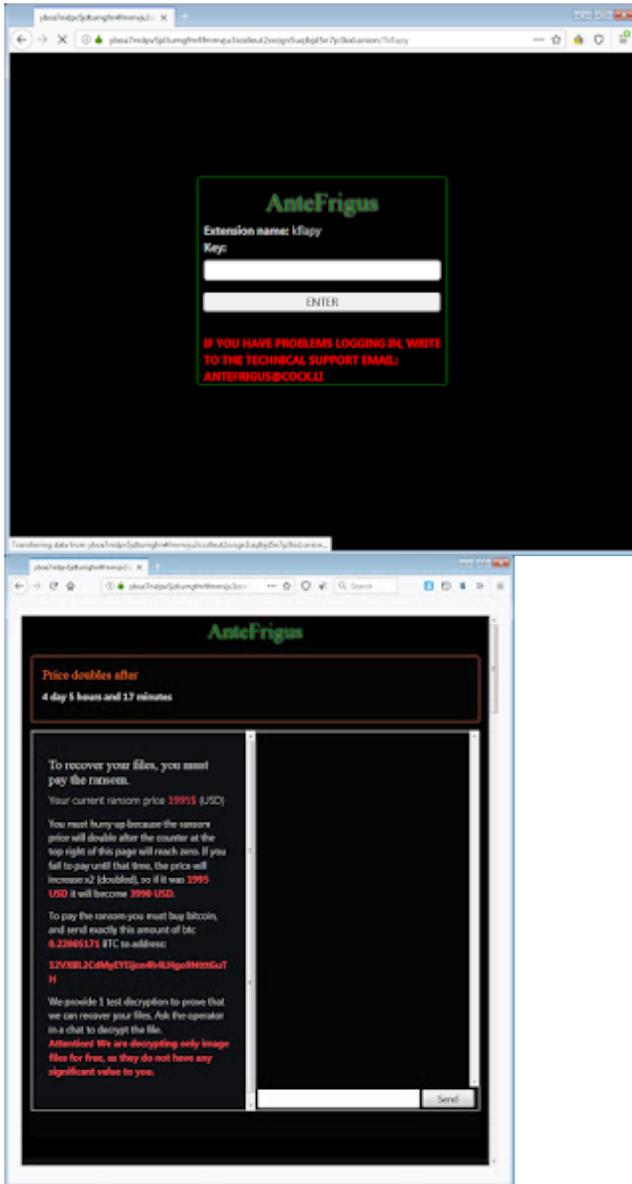
!!!!!!!ЕЩЕ РАЗ: В ваших интересах вернуть ваши файлы. Со своей стороны мы (лучшие специалисты) делаем все для восстановления, но, пожалуйста, не мешайте.

!!!!!!!

---

Записка о выкупе также сохраняется в специальной папке на диске C:  
C:\Instraction\

Скриншоты сайта вымогателей:



## Технические детали

Распространяется с помощью вредоносной рекламной кампании HookAds, вредоносная реклама которой теперь перенаправляет пользователей на веб-страницы с набором эксплойтов RIG. На инфицированном ПК разворачивается вредоносный элемент, который устанавливает шифровальщик **AnteFrigus**. В 2018 году HookAds распространяла GlobeImposter. На момент написания этой статьи рекламная кампания HookAds уже продолжается несколько лет (с 2016 года), и каждый день регистрируются новые мошеннические рекламные домены.

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов (RIG EK), вредоносной рекламы, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).

**i** 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.

➤ В отличие от других вымогателей, AnteFrigus не предназначен для диска "C", а только для других дисков, в описанном примере его целями были съемные устройства и подключенные сетевые диски (буквы дисков из кода D:, E:, F:, G:, H:, I:).

```
492 sub_409597(&v90);
493 drive_parse(v43, L"E:");
494 LOBYTE(v81) = '0';
495 drive_parse(v44, L"D:");
496 LOBYTE(v81) = '1';
497 drive_parse(v45, L"F:");
498 LOBYTE(v81) = '2';
499 drive_parse(v46, L"I:");
500 LOBYTE(v81) = '3';
501 drive_parse(v47, L"U:");
502 LOBYTE(v81) = 52;
503 drive_parse(v48, L"G:");
504 LOBYTE(v81) = 53;
505 drive_parse(v49, L"H:");
506 LOBYTE(v81) = 54;
507 v50 = sub_43E3A7(8);
```

➤ Для определения IP ПК используется сайт:  
[xxxx://iplog.org/10UJ73](http://iplog.org/10UJ73)

### Список файловых расширений, подвергающихся шифрованию:

Все файлы, кроме пропускаемых.

Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

### Пропускаемые типы файлов:

.adv, .ani, .bat, .big, .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, .pck, .prf, .rom, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .wpx (49 расширений).

### Файлы, связанные с этим Ransomware:

<random>-readme.txt - шаблон записки

hssjyh-readme.txt - пример записки  
test.txt - файл для блокировки или отладки.  
rad26628.tmp.exe - пример названия вредоносного файла  
<random>.tmp.exe - шаблон названия вредоносного файла

### Расположения:

C:\Instraction\  
\Desktop\ ->  
\User\_folders\ ->  
\%TEMP%\ ->

### Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

### Сетевые подключения и связи:

Tor-URL: xxxx://yboa7nidpv5jdtumgfm4fmmvju3ccxlleut2xvzgn5uqlbjd5n7p3kid.onion/

Email: antefrigus@cock.li

BTC: -

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

### Результаты анализов:

Ⓜ [Hybrid analysis >>](#)

Σ

 [Intezer analysis >>](#)

⌘ [ANY.RUN analysis >>](#)

⊗ [VMRay analysis >>](#)

Ⓟ [VirusBay samples >>](#)

☐ [MalShare samples >>](#)

👁 [AlienVault analysis >>](#)

🔄 [CAPE Sandbox analysis >>](#)

🔗 [JOE Sandbox analysis >>](#)

Степень распространённости: низкая.

Подробные сведения собираются регулярно. Присылайте образцы.

---

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

---

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

### Обновление от 10 февраля 2020:

[Пост в Твиттере >>](#)

Расширения: .eaaaae, .bbadc



can't access the download page of the TOR browser, then download the VPN!

After you install the TOR browser on your computer go to the site:

<http://i6jppiczqa5moqfl57gssi33npwfseqppdsnz7rriiv7suf4pf4w42id.onion>

After going to the site, enter the information:

Your ID: 32476\*\*\*\*\*

Personal key:

a2hobG1qKGhrdHB1KDo5Oz49OTk4PTcoSkEnOTw8Njk5OCdOaUM2a\*\*\*\*\*==

Your Email

**Обновление от 19 января 2020:**

Результаты анализов: [VT](#) + [IA](#)

---

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



Thanks :

GrujaRS, mol69, Michael Gillespie, Lawrence Abrams

Andrew Ivanov (author), Emmanuel\_ADC-Soft, S!Ri

\*\*\*

to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles.