New Satan Ransomware available through a Ransomware as a Service.

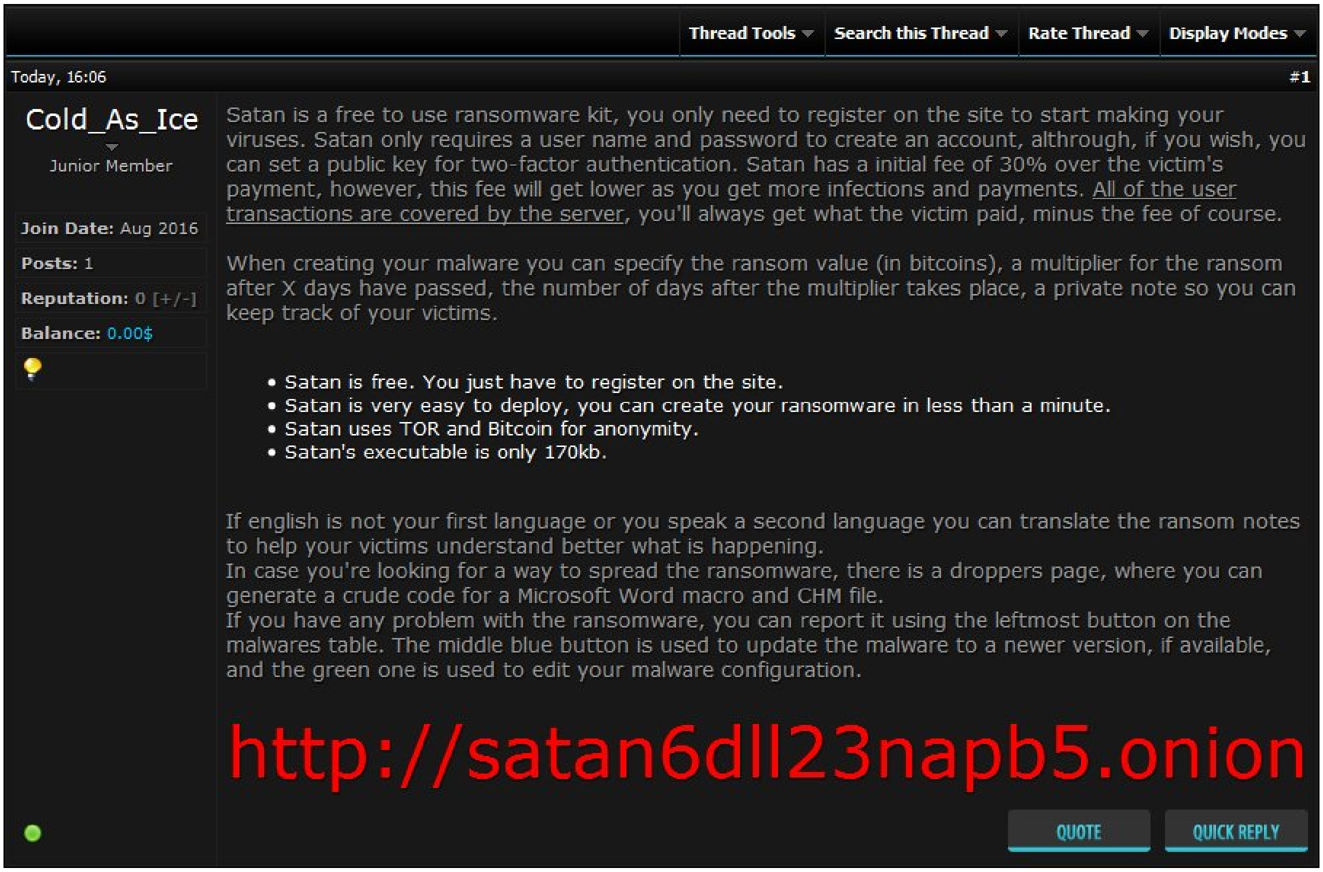
bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-

By
Lawrence Abrams

- January 19, 2017
- 03:10 PM
- 5

A new Ransomware as a Service, or RaaS, called Satan has been discovered by security researcher Xylitol. This service allows any wannabe criminal to register an account and create their very own customized version of the Satan Ransomware.

Once the ransomware is created, it is then up to the criminal to determine how they will distribute the ransomware, while the RaaS will handle the ransom payments and adding new features. For this service, the RaaS developer takes a 30% cut of any payments that are made by victims. According to the advertisement for the Satan RaaS, the developer will reduce their cut depending on the volume of payments received by an affiliate.



Today, 16:06 #1

Cold_As_Ice
Junior Member

Join Date: Aug 2016
Posts: 1
Reputation: 0 [+/-]
Balance: 0.00$

Satan is a free to use ransomware kit, you only need to register on the site to start making your viruses. Satan only requires a user name and password to create an account, althrough, if you wish, you can set a public key for two-factor authentication. Satan has a initial fee of 30% over the victim's payment, however, this fee will get lower as you get more infections and payments. All of the user transactions are covered by the server, you'll always get what the victim paid, minus the fee of course.

When creating your malware you can specify the ransom value (in bitcoins), a multiplier for the ransom after X days have passed, the number of days after the multiplier takes place, a private note so you can keep track of your victims.

- Satan is free. You just have to register on the site.
- Satan is very easy to deploy, you can create your ransomware in less than a minute.
- Satan uses TOR and Bitcoin for anonymity.
- Satan's executable is only 170kb.

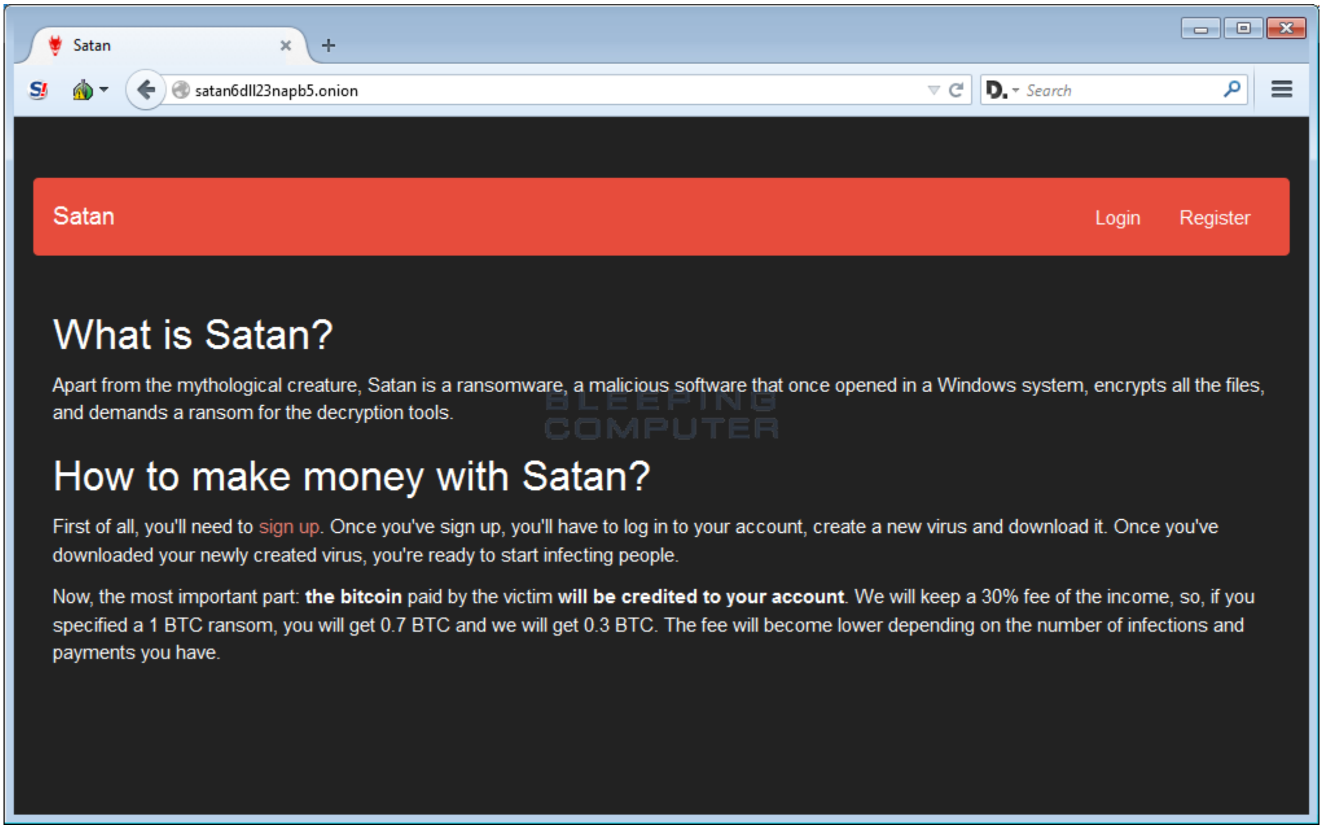
If english is not your first language or you speak a second language you can translate the ransom notes to help your victims understand better what is happening.
In case you're looking for a way to spread the ransomware, there is a droppers page, where you can generate a crude code for a Microsoft Word macro and CHM file.
If you have any problem with the ransomware, you can report it using the leftmost button on the malwares table. The middle blue button is used to update the malware to a newer version, if available, and the green one is used to edit your malware configuration.

http://satan6dll23napb5.onion

Promoting on Underground Web Sites
Source: Xylitol

The Satan RaaS

When a person first goes to the Satan RaaS they will be greeted with a home page that describes what the service is and how a criminal can make money with it.



What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

How to make money with Satan?

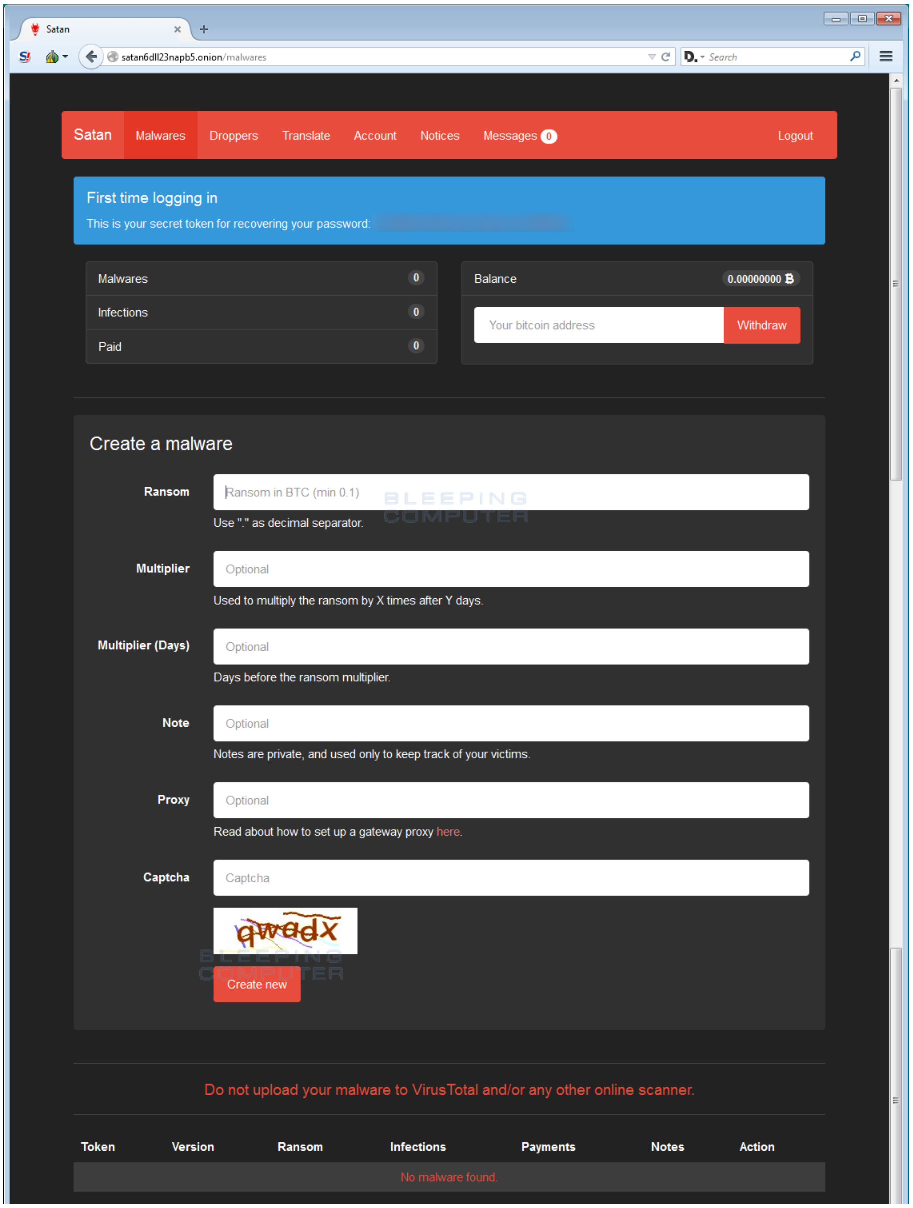
First of all, you'll need to sign up. Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.

Satan RaaS Home Page

Once a user registers an account and logs in, they will be greeted with an affiliate console that contains various pages that they can use to help distribute their ransomware. These pages are the Malwares, Droppers, Translate, Account, Notices, and Messages pages.

The first page that is shown when someone logs in is the **Malwares** page, which allows a criminal to configure various settings of their very customized version of the Satan Ransomware. In terms of customization, there is not really many options. A user can specify the ransom amount, how much it goes up after a certain amount of the days, and the amount of days that the ransom payment should increase.



First time logging in

This is your secret token for recovering your password: [redacted]

Malwares	0
Infections	0
Paid	0

Balance 0.00000000 Ƀ

Your bitcoin address | Withdraw

Create a malware

Ransom: Ransom in BTC (min 0.1)
Use "." as decimal separator.

Multiplier: Optional
Used to multiply the ransom by X times after Y days.

Multiplier (Days): Optional
Days before the ransom multiplier.

Note: Optional
Notes are private, and used only to keep track of your victims.

Proxy: Optional
Read about how to set up a gateway proxy here.

Captcha: Captcha

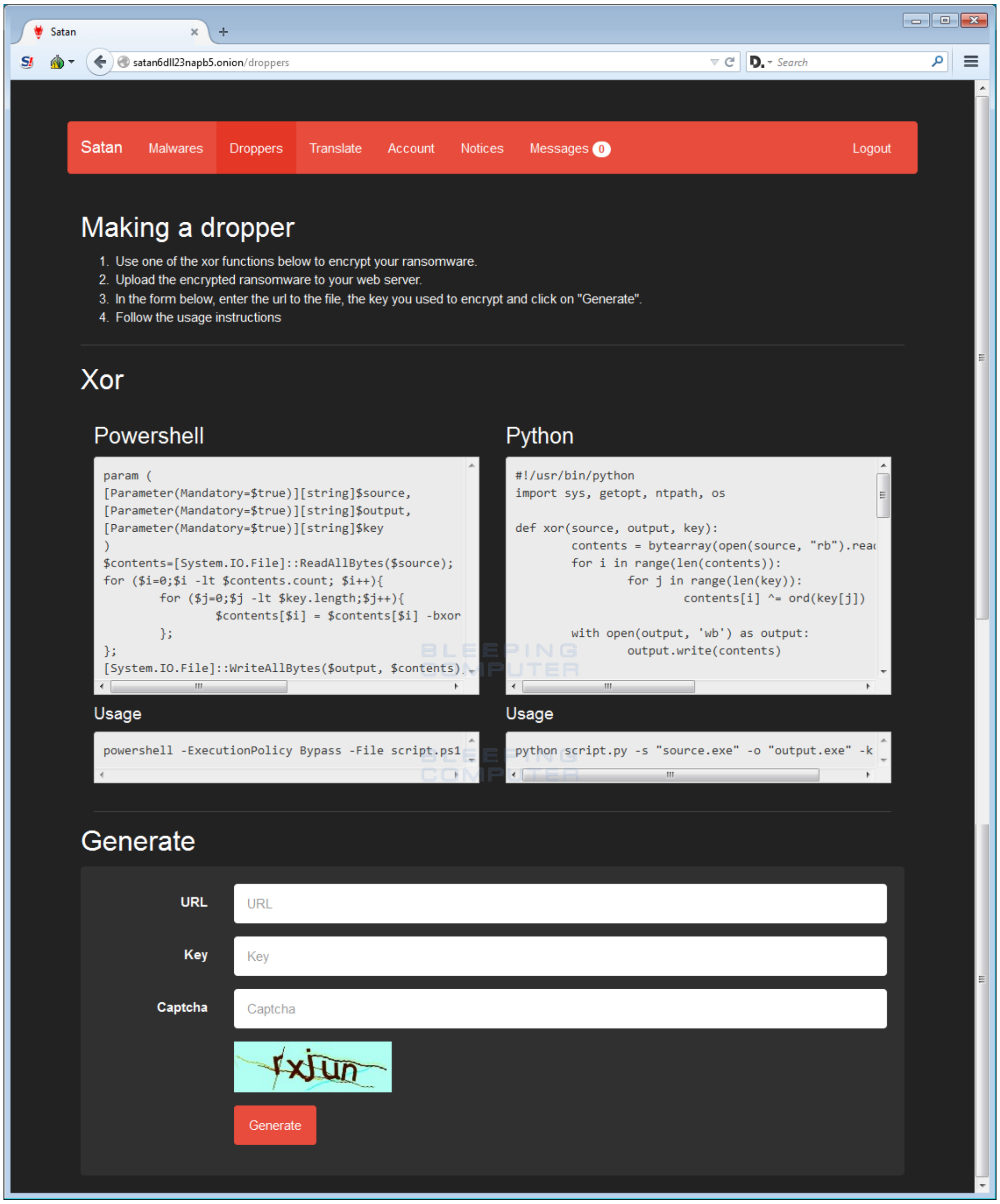
Do not upload your malware to VirusTotal and/or any other online scanner.

Token	Version	Ransom	Infections	Payments	Notes	Action
No malware found.						

Satan RaaS Ransomware Generation Page

The **Droppers** page, shown below, provides code that assists the affiliate in creating malicious Microsoft Word macros or CHM installers. These can then be used by the affiliate to distribute the ransomware via SPAM or other means.

This the first time I have seen a public RaaS like this offer tips and help to the affiliates when it comes to distribution methods. This type of hand holding could allow a curious affiliate to become an active one.



Making a dropper

1. Use one of the xor functions below to encrypt your ransomware.
2. Upload the encrypted ransomware to your web server.
3. In the form below, enter the url to the file, the key you used to encrypt and click on "Generate".
4. Follow the usage instructions

Xor

Powershell

```
param (
[Parameter(Mandatory=$true)][string]$source,
[Parameter(Mandatory=$true)][string]$output,
[Parameter(Mandatory=$true)][string]$key
)
$contents=[System.IO.File]::ReadAllBytes($source);
for ($i=0;$i -lt $contents.count; $i++){
        for ($j=0;$j -lt $key.length;$j++){
                $contents[$i] = $contents[$i] -bxor
        };
};
[System.IO.File]::WriteAllBytes($output, $contents).
```

Usage

```
powershell -ExecutionPolicy Bypass -File script.ps1
```

Python

```
#!/usr/bin/python
import sys, getopt, ntpath, os

def xor(source, output, key):
        contents = bytearray(open(source, "rb").reac
        for i in range(len(contents)):
                for j in range(len(key)):
                        contents[i] ^= ord(key[j])

        with open(output, 'wb') as output:
                output.write(contents)
```

Usage

```
python script.py -s "source.exe" -o "output.exe" -k
```

Generate

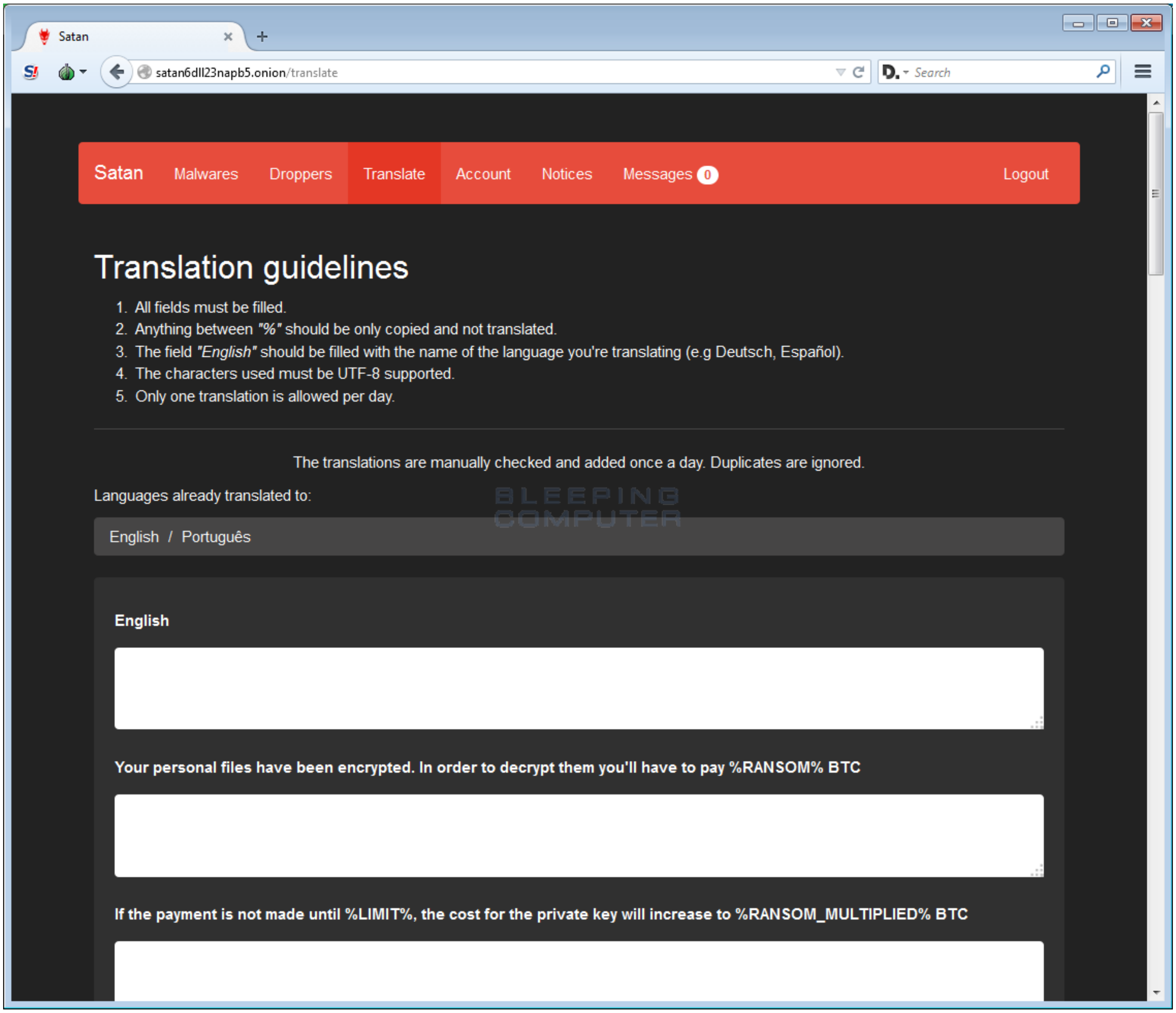
URL: URL

Key: Key

Captcha: Captcha

Satan RaaS Droppers Page

The **Translate** page allows affiliates to expand the languages used by Satan for the ransom notes.



Translation guidelines

1. All fields must be filled.
2. Anything between *"%"* should be only copied and not translated.
3. The field *"English"* should be filled with the name of the language you're translating (e.g Deutsch, Español).
4. The characters used must be UTF-8 supported.
5. Only one translation is allowed per day.

The translations are manually checked and added once a day. Duplicates are ignored.

Languages already translated to:

English / Português

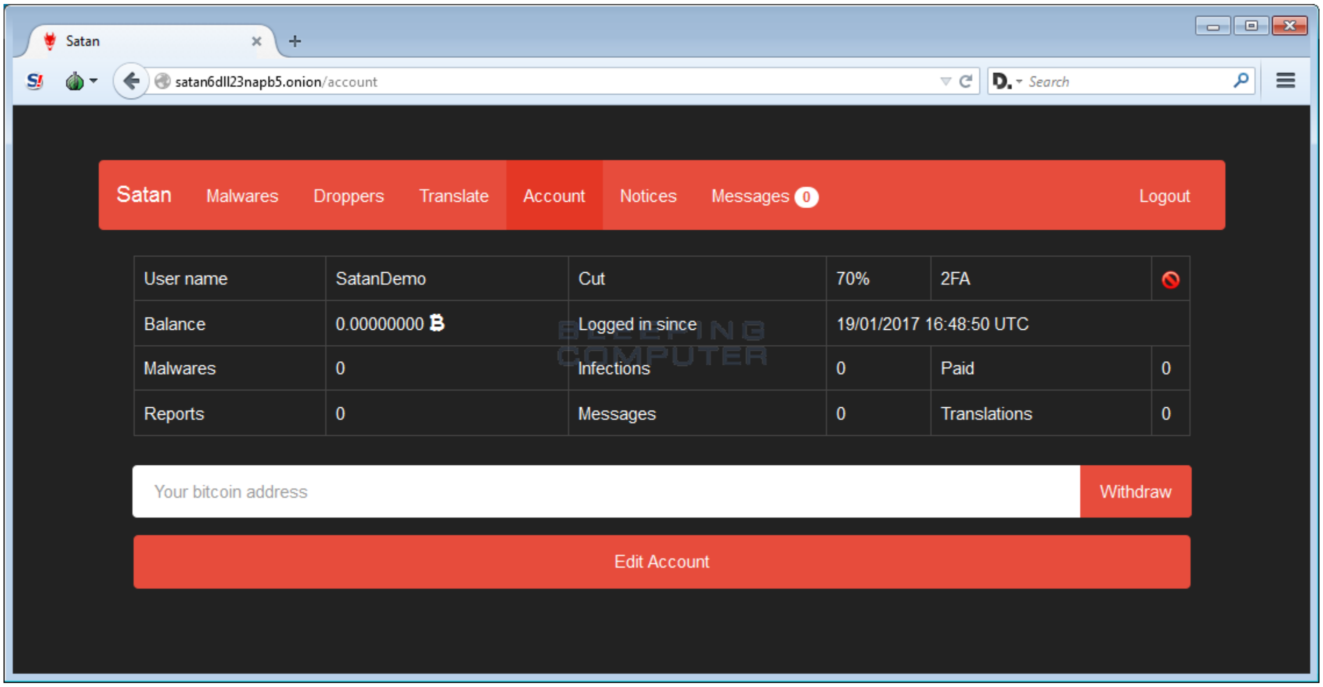
English

Your personal files have been encrypted. In order to decrypt them you'll have to pay %RANSOM% BTC

If the payment is not made until %LIMIT%, the cost for the private key will increase to %RANSOM_MULTIPLIED% BTC

Satan RaaS Translation Page

The **Account** page is where the affiliate can see the amount of people infected, the amount paid, and other information.



User name	SatanDemo	Cut	70%	2FA	🚫
Balance	0.00000000 Ƀ	Logged in since	19/01/2017 16:48:50 UTC		
Malwares	0	Infections	0	Paid	0
Reports	0	Messages	0	Translations	0

Satan RaaS Account Information Page

Finally there is a **Notices** page, which will be used to display messages from the RaaS developer, and a **Messages** page that can be used for "customer service" requests.

As for the Satan Ransomware Itself...

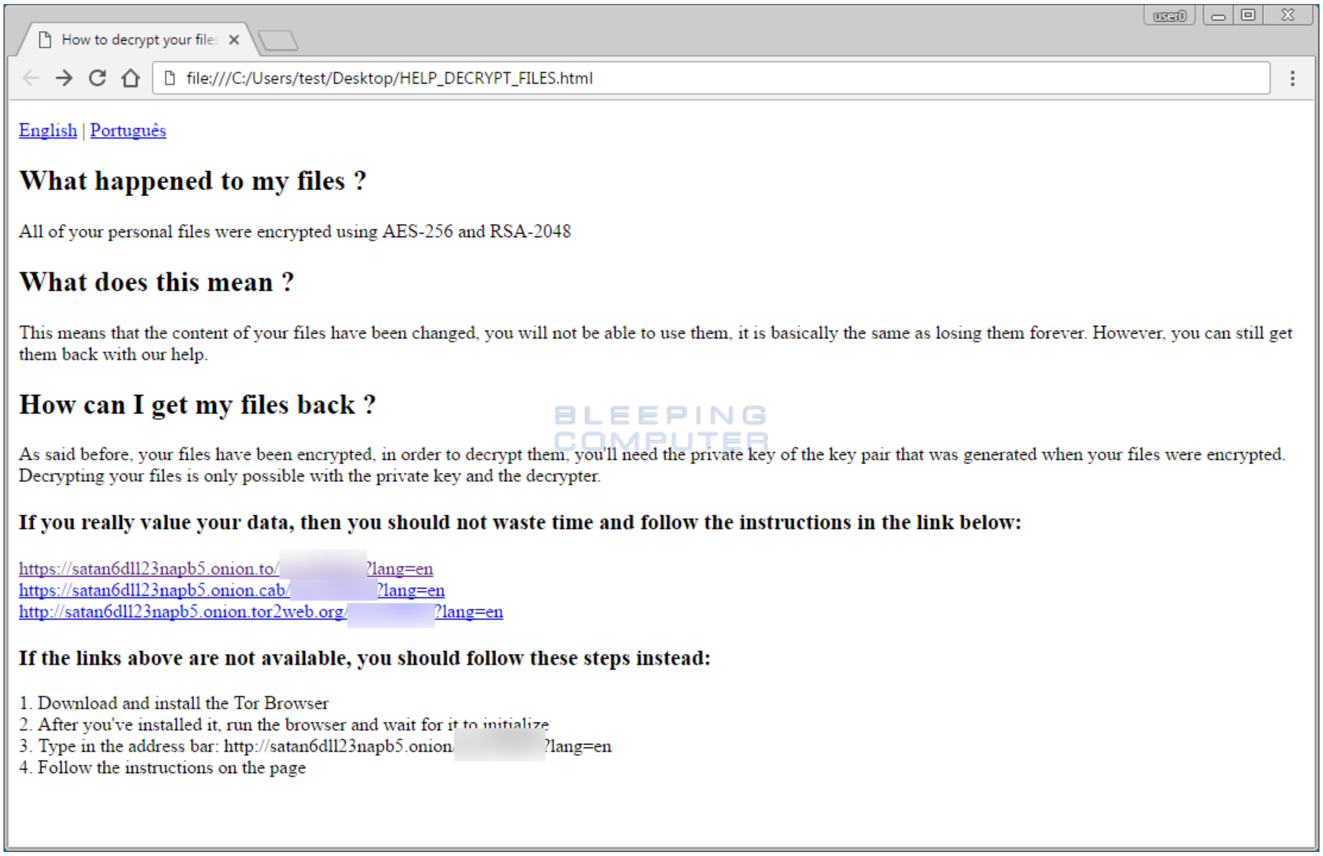
When the Satan Ransomware is installed it will check to see if it is running under a virtual machine, and if it is, will terminate. Once executed it will inject itself into TaskHost.exe and begin to encrypt the data on the computer. It is currently unknown what encryption algorithm Satan uses, but it will target files with the following extensions:

```
.incpas, .mp4, .pab, .st6, .sas7bdat, .wmv, .backup, .drf, .ibank, .3ds, .odg, .cer,
.tif, .cs, .dotx, .7z, .png, .bak, .ibz, .db3, .pbl, .3fr, .dxf, .nk2, .bkp, .mdf,
.svg, .xlm, .3dm, .pct, .java, .pot, .sxi, .ibd, .sxw, .pspimage, .ppt, .kbx, .ppsm,
.ndd, .txt, .pdb, .say, .backupdb, .fla, .swf, .asx, .accdt, .mp3, .ycbcra, .erf,
.cr2, .pfx, .potx, .qby, .sqlite, .blend, .class, .pat, .odp, .gray, .qbw, .tib,
.thm, .htm, .mos, .rm, .key, .std, .tlg, .lua, .pst, .sqlitedb, .grey, .cdr4, .dc2,
.ce1, .ps, .tex, .eml, .xlam, .pages, .st8, .jar, .st7, .potm, .sdf, .db-journal,
.pcd, .aspx, .rwl, .kpdx, .fmb, .xlr, .gry, .kc2, .oil, .moneywell, .xlk, .sti,
.accdr, .oth, .c, .xml, .nd, .mdb, .pem, .erbsql, .bpw, .ffd, .ost, .pptm, .dwg,
.zip, .qbm, .cdx, .des, .dng, .pdd, .cfp, .nyf, .cgm, .sldm, .xla, .odf, .raf, .crw,
.mef, .raw, .x11, .nsd, .fff, .design, .dcs, .ptx, .al, .ns2, .bik, .back, .accdb,
.nwb, .cpi, .ads, .odt, .sqlite3, .docm, .drw, .pl, .nx2, .fpx, .rdb, .otp, .msg,
.accde, .agdl, .php, .csv, .py, .rtf, .ach, .sda, .ddd, .asf, .dotm, .cmt, .h, .hbk,
.xlsx, .s3db, .tga, .wav, .iif, .dxb, .sql, .db, .sd0, .bgt, .djvu, .jpg, .doc,
.craw, .mpg, .sxd, .kdc, .jpeg, .psafe3, .flac, .dtd, .act, .qba, .vob, .cdrw, .eps,
.bkf, .mdc, .rar, .mov, .cdf, .m4v, .ab4, .bank, .pps, .cib, .dot, .dgc, .exf, .flv,
.xlsb, .ddrw, .adb, .srw, .plc, .csh, .xls, .fxg, .otg, .pas, .xlt, .indd, .rwz,
.xltx, .apj, .stw, .xltm, .orf, .ott, .qbb, .max, .cls, .obj, .docx, .dcr, .cdr3,
.qbx, .pdf, .nef, .ots, .srt, .ddoc, .rat, .phtml, .m, .dbx, .nxl, .avi, .p12, .awg,
.dbf, .ns3, .mmw, .prf, .wallet, .rw2, .jin, .odc, .qbr, .ppsx, .ns4, .wpd, .wps,
.nsh, .dxg, .fhd, .dac, .wb2, .nrw, .odb, .ait, .jpe, .odm, .sldx, .fdb, .acr, .war,
.oab, .sxc, .cpp, .r3d, .hpp, .asm, .st5, .stx, .xis, .dds, .xlsm, .p7c, .cdr5, .3g2,
.mrw, .sr2, .html, .cdr, .idx, .st4, .bdb, .kdbx, .nsg, .der, .ods, .myd, .nop,
.ppam, .pptx, .yuv, .xlw, .mfw, .nsf, .csl, .php5, .p7b, .crt, .asp, .srf, .jsp,
.cdr6, .sxm, .iiq, .3gp, .ce2, .arw, .bay, .ai, .sxg, .psd, .3pr, .fh, .pef, .x3f,
.sik, .bpp, .vmdk, .spi, .bup, .cvt, .bb, .fkc, .tjl, .dbk, .swp, .fb, .vib, .dtb,
.bke, .old, .bkc, .jou, .rpb, .abk, .sav, .bkn, .tbk, .fbw, .vrb, .spf, .bk, .sbk,
.umb, .ac, .vbk, .wbk, .mbk
```

When it has encrypted a file, it will scramble its name and append the **.stn** extension to the file. For example, test.jpg may become ahasd.stn. While encrypting files it will also create a ransom note called HELP_DECRYPT_FILES.html in each folder that a file has been encrypted.

When it has finished encrypting the computer, it will execute the **C:\Windows\System32\cipher.exe" /W:C** command to wipe all data from the unused space on the C: Drive.

Finally it will display the ransom note, which contains a unique victim ID and a URL to a TOR payment site.


How to decrypt your file:
file:///C:/Users/test/Desktop/HELP_DECRYPT_FILES.html

English | Português

What happened to my files ?

All of your personal files were encrypted using AES-256 and RSA-2048

What does this mean ?

This means that the content of your files have been changed, you will not be able to use them, it is basically the same as losing them forever. However, you can still get them back with our help.

How can I get my files back ?

As said before, your files have been encrypted, in order to decrypt them, you'll need the private key of the key pair that was generated when your files were encrypted. Decrypting your files is only possible with the private key and the decrypter.

If you really value your data, then you should not waste time and follow the instructions in the link below:

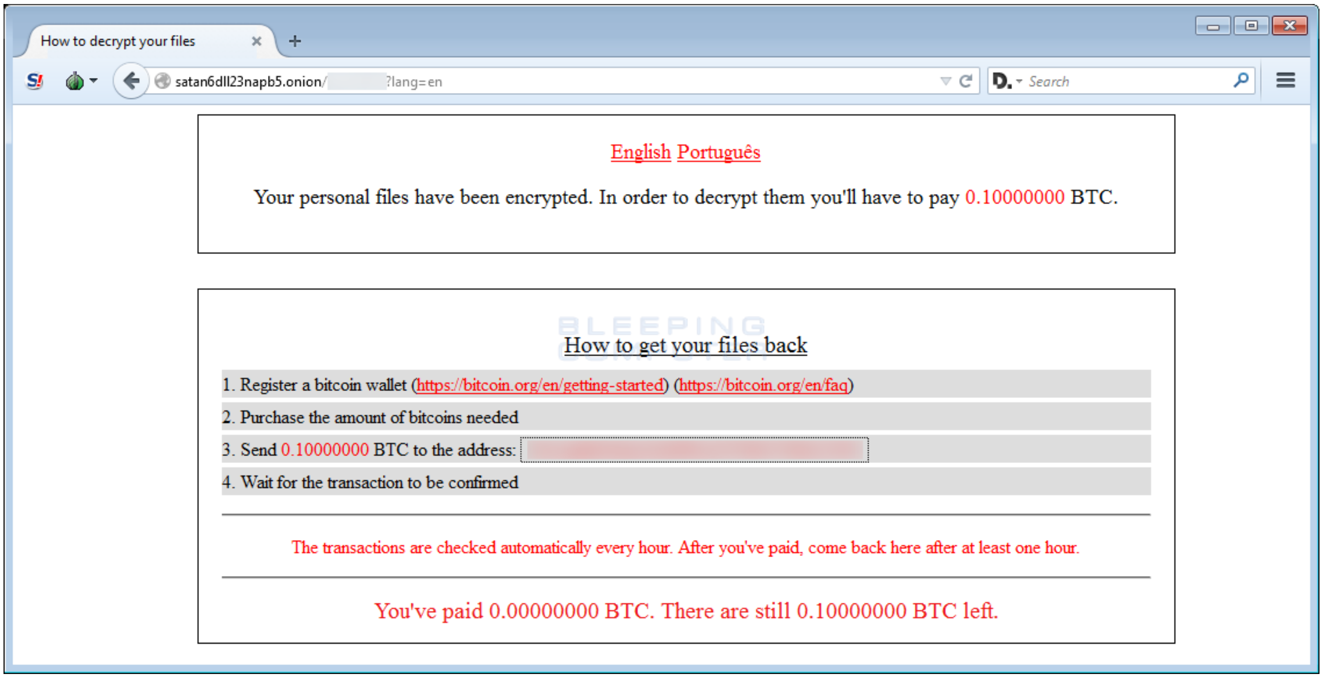
https://satan6dll23napb5.onion.to/[redacted]?lang=en
https://satan6dll23napb5.onion.cab/[redacted]?lang=en
http://satan6dll23napb5.onion.tor2web.org/[redacted]?lang=en

If the links above are not available, you should follow these steps instead:

1. Download and install the Tor Browser
2. After you've installed it, run the browser and wait for it to initialize
3. Type in the address bar: http://satan6dll23napb5.onion[redacted]?lang=en
4. Follow the instructions on the page

Satan Ransomware Ransom Note

When a victim clicks on one of the enclosed URLs they will be brought to Satan's payment site where they can get payment instructions.


How to decrypt your files
satan6dll23napb5.onion/[redacted]?lang=en
Search

English Português

Your personal files have been encrypted. In order to decrypt them you'll have to pay 0.10000000 BTC.

How to get your files back

1. Register a bitcoin wallet (https://bitcoin.org/en/getting-started) (https://bitcoin.org/en/faq)
2. Purchase the amount of bitcoins needed
3. Send 0.10000000 BTC to the address: [redacted]
4. Wait for the transaction to be confirmed

The transactions are checked automatically every hour. After you've paid, come back here after at least one hour.

You've paid 0.00000000 BTC. There are still 0.10000000 BTC left.

Satan Ransomware Payment Site

Unfortunately, at this time there is no way to decrypt the files for free. For those who wish to discuss this ransomware or receive support, you can use our dedicated help topic: Satan Ransomware Help & Support Topic.

Associated Satan Ransomware Files:

```
HELP_DECRYPT_FILES.html
```

Network Communication:

```
https://ejmv6pxsuwqrofa3.onion.to
https://satan6dll23napb5.onion.to
https://satan6dll23napb5.onion.cab
http://satan6dll23napb5.onion.tor2web.org
satan6dll23napb5.onion
```

Hashes:

```
SHA256: c04836696d715c544382713eebf468aeff73c15616e1cd8248ca8c4c7e931505
```

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

- RaaS
- Ransomware
- Satan

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-
  MihailProg - 5 years ago

  Looks cool, it's well made and it's a good idea.
  I hope this works out for them and they make a lot of money.

-
  Almarma - 5 years ago

  "Looks cool, it's well made and it's a good idea.
  I hope this works out for them and they make a lot of money."

  You must be kidding, right? Even more ransomware? No, thanks. And I wish you become a victim yourself, so we can see if you find it that funny afterwards ¬¬

-
  mikeloeven - 5 years ago

  Its really sad that ransomware has become such an effective tool for criminals considering that its super easy to defeat. all you need is an external hot swap bay and a schedule to rotate out your backup drives so you always have a up to date copy of your drive images offline heck even the most computer illiterate person can subscribe to and configure cloud storage through most commercially available backup software.

-

  whyder - 5 years ago

  We got hit and paid the ransom. The decrypter does nothing. Doesn't decrypt anything. Do not pay

-

  BitCoinMember - 4 years ago

  Kann ich BItte einen Decrypter für die *stn Dateien bekommen.
  Bräuchte dringend Hilfe

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: