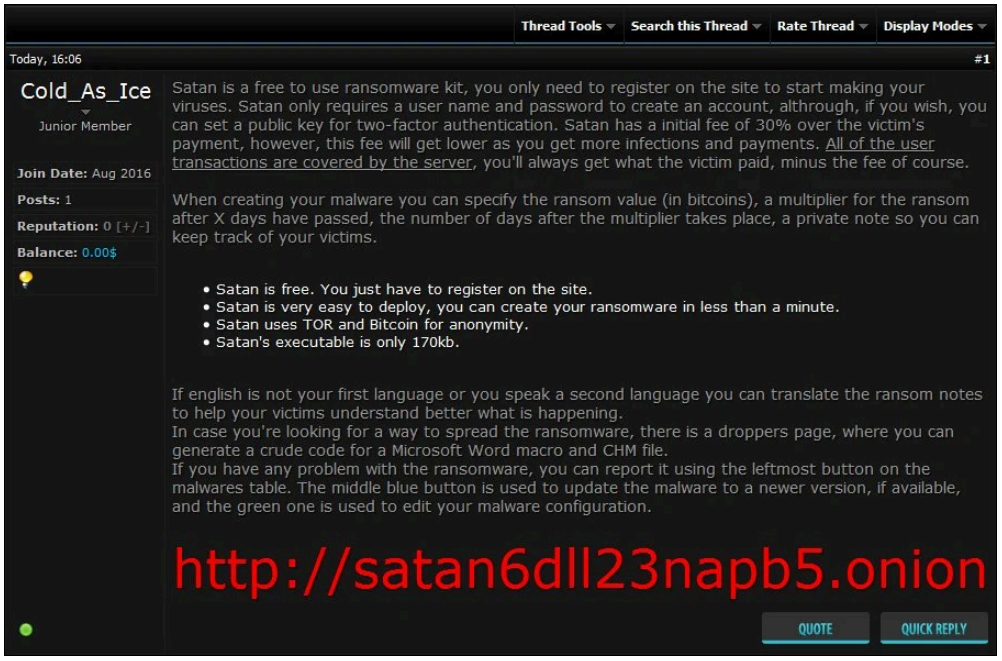
New Satan Ransomware available through a Ransomware as a Service.

By Lawrence Abrams

Published: 2017-01-19 · Archived: 2026-04-05 19:15:55 UTC

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.

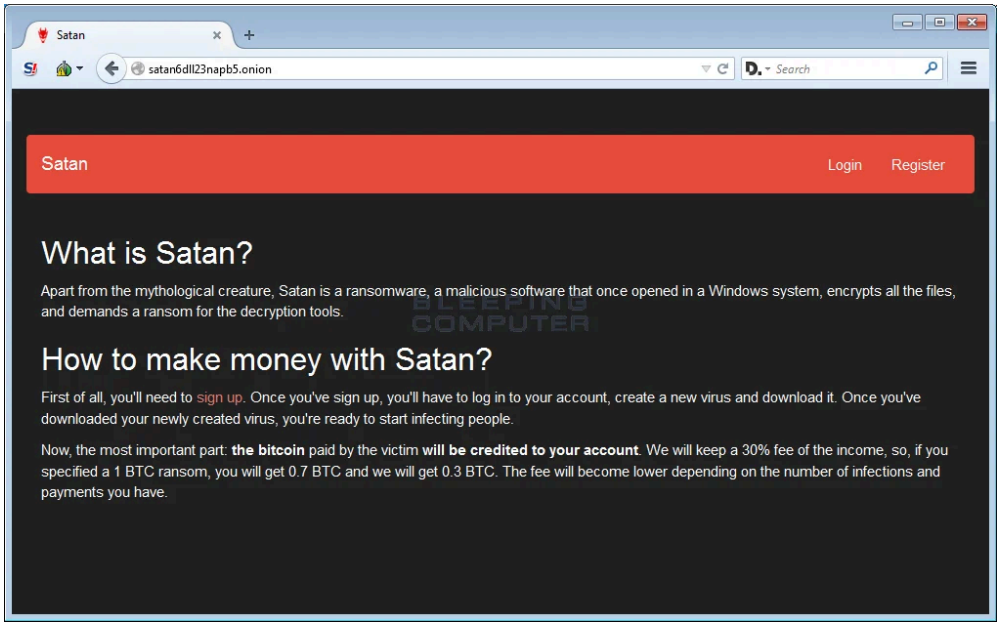
Once the ransomware is created, it is then up to the criminal to determine how they will distribute the ransomware, while the RaaS will handle the ransom payments and adding new features. For this service, the RaaS developer takes a 30% cut of any payments that are made by victims. According to the advertisement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



Promoting on Underground Web Sites
Source: Xylitol

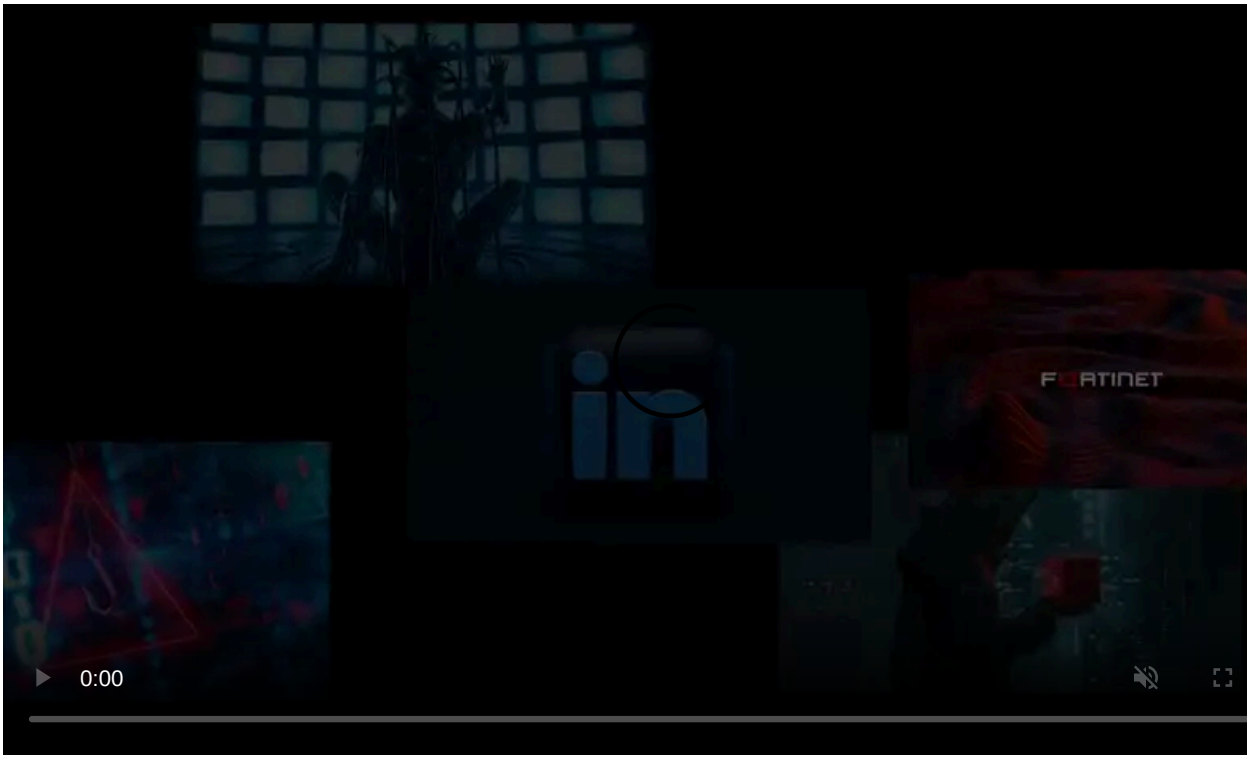
The Satan RaaS

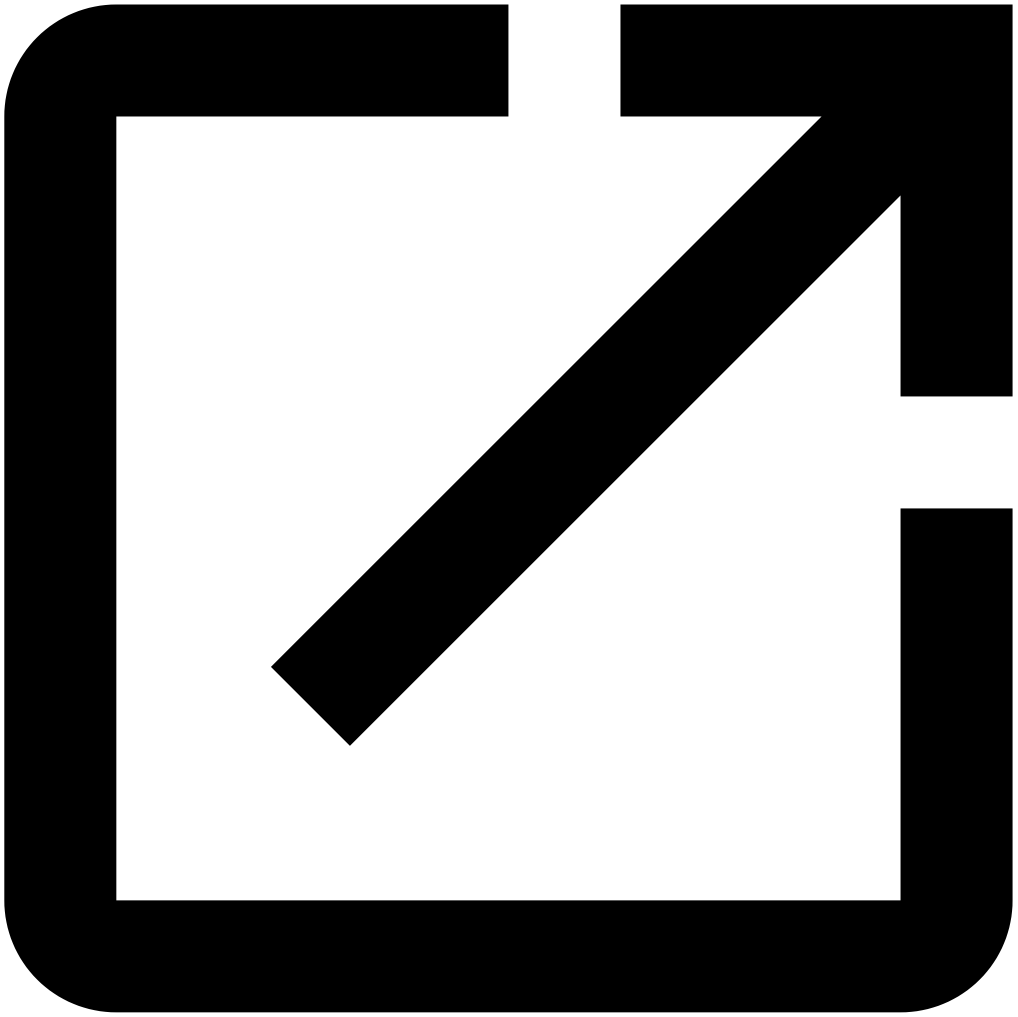
When a person first goes to the Satan RaaS they will be greeted with a home page that describes what the service is and how a criminal can make money with it.



Satan RaaS Home Page

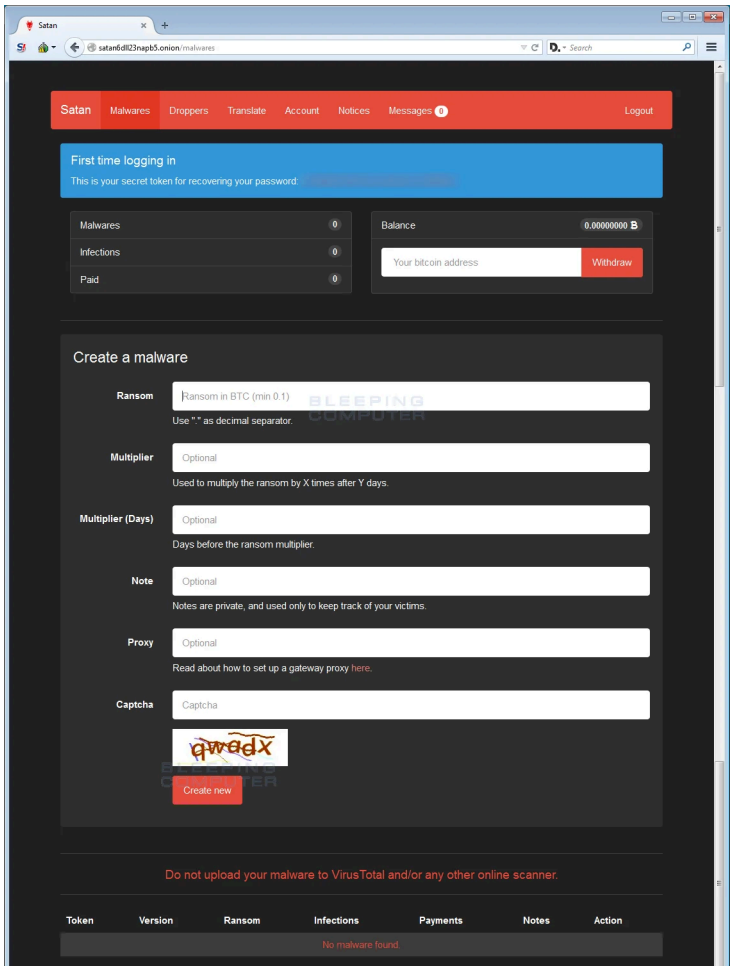
Once a user registers an account and logs in, they will be greeted with an affiliate console that contains various pages that they can use to help distribute their ransomware. These pages are the Malwares, Droppers, Translate, Account, Notices, and Messages pages.


0:00



Visit Advertiser websiteGO TO PAGE

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.



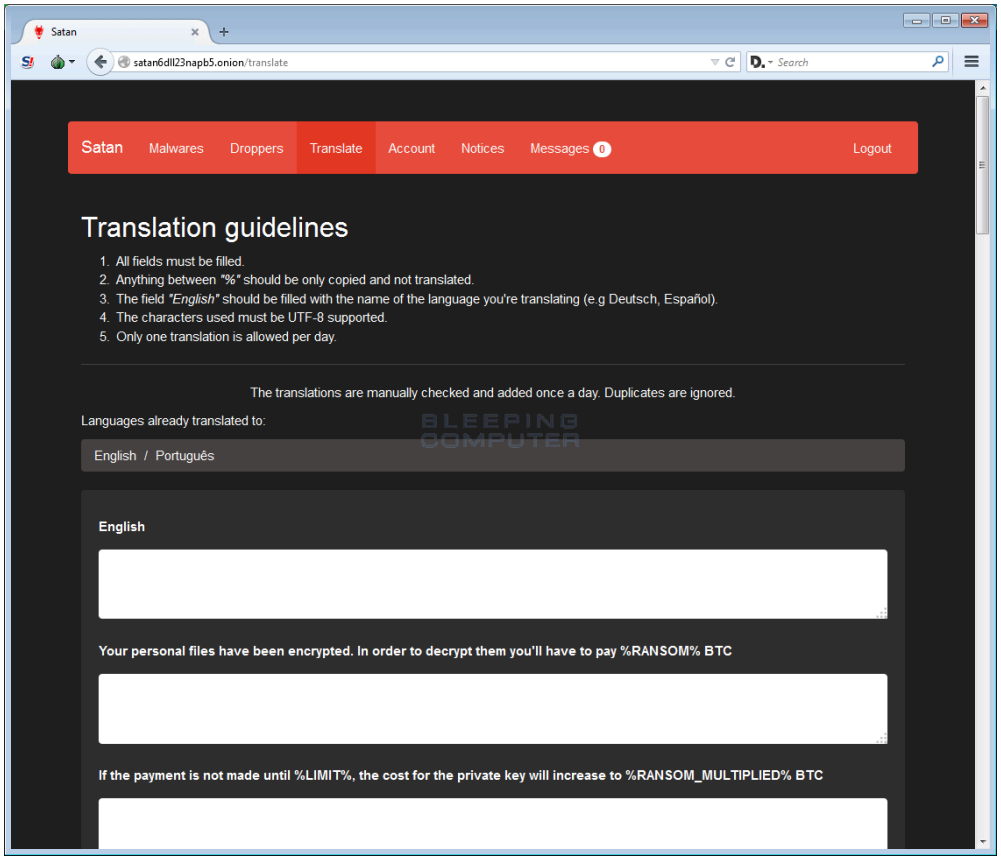
Satan RaaS Ransomware Generation Page

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.

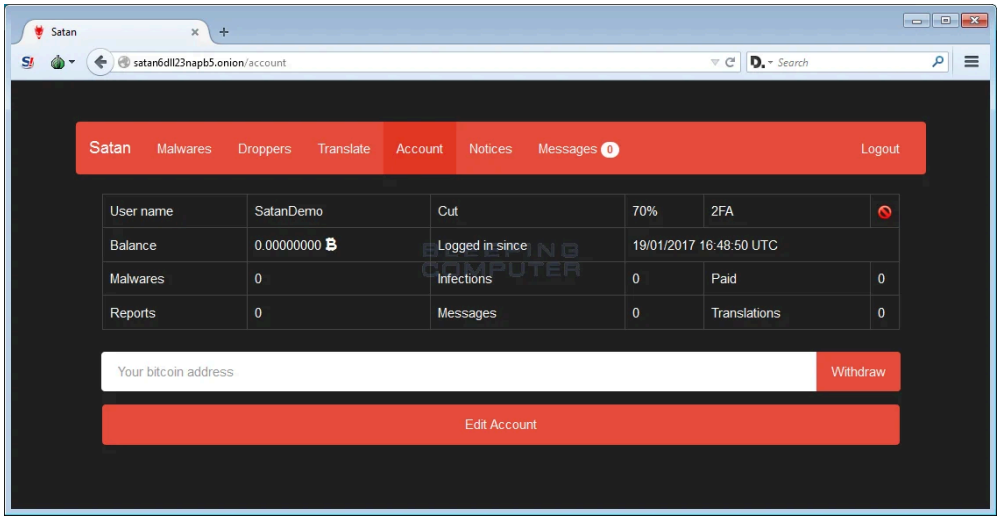
Satan RaaS Droppers Page

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



Satan RaaS Translation Page

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



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,
```

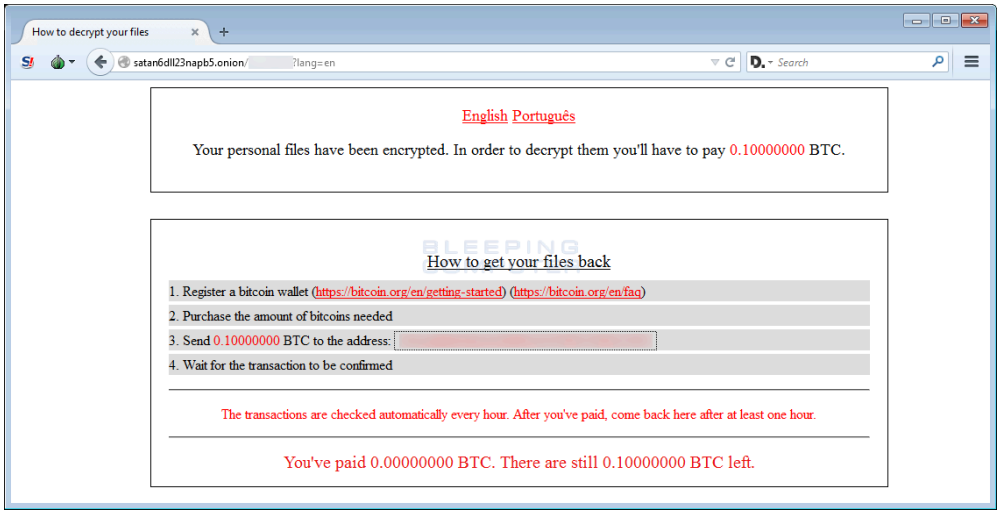
When it has encrypted a file, it will scramble its name and append the **.stn** extension to the file. For example, test.jpg may become ahasd.stn. While encrypting files it will also create a ransom note called HELP_DECRYPT_FILES.html in each folder that a file has been encrypted.

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.

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.



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:

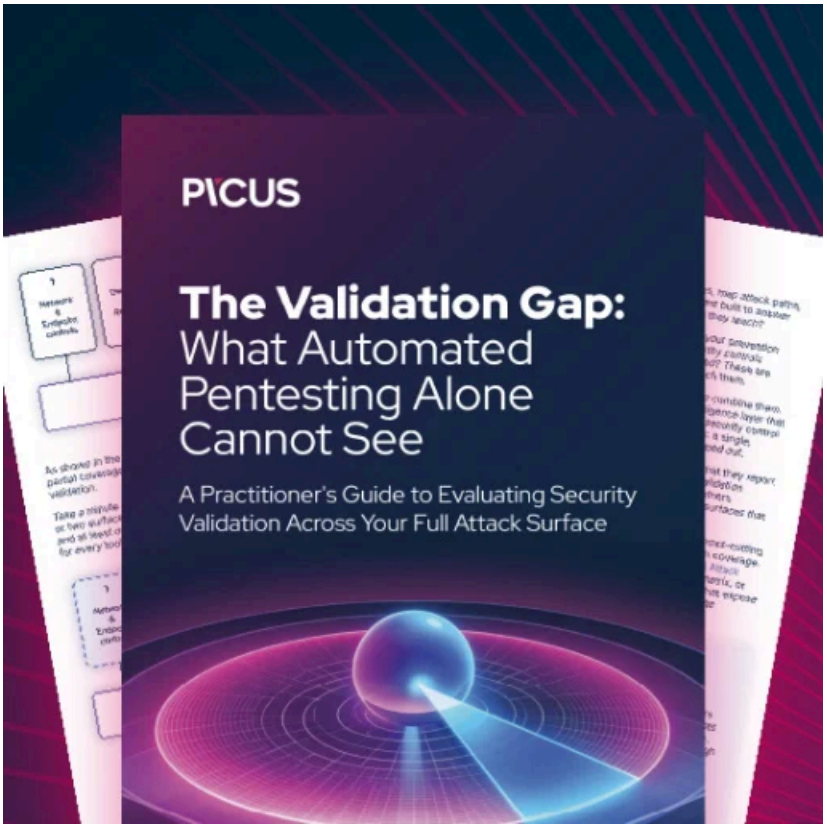
```
HELP_DECRYPT_FILES.html
```

Network Communication:

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

Hashes:

```
SHA256: c04836696d715c544382713eebf468aeff73c15616e1cd8248ca8c4c7e931505
```



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/