New tool Shifr RaaS allows anyone to create ransomware easily

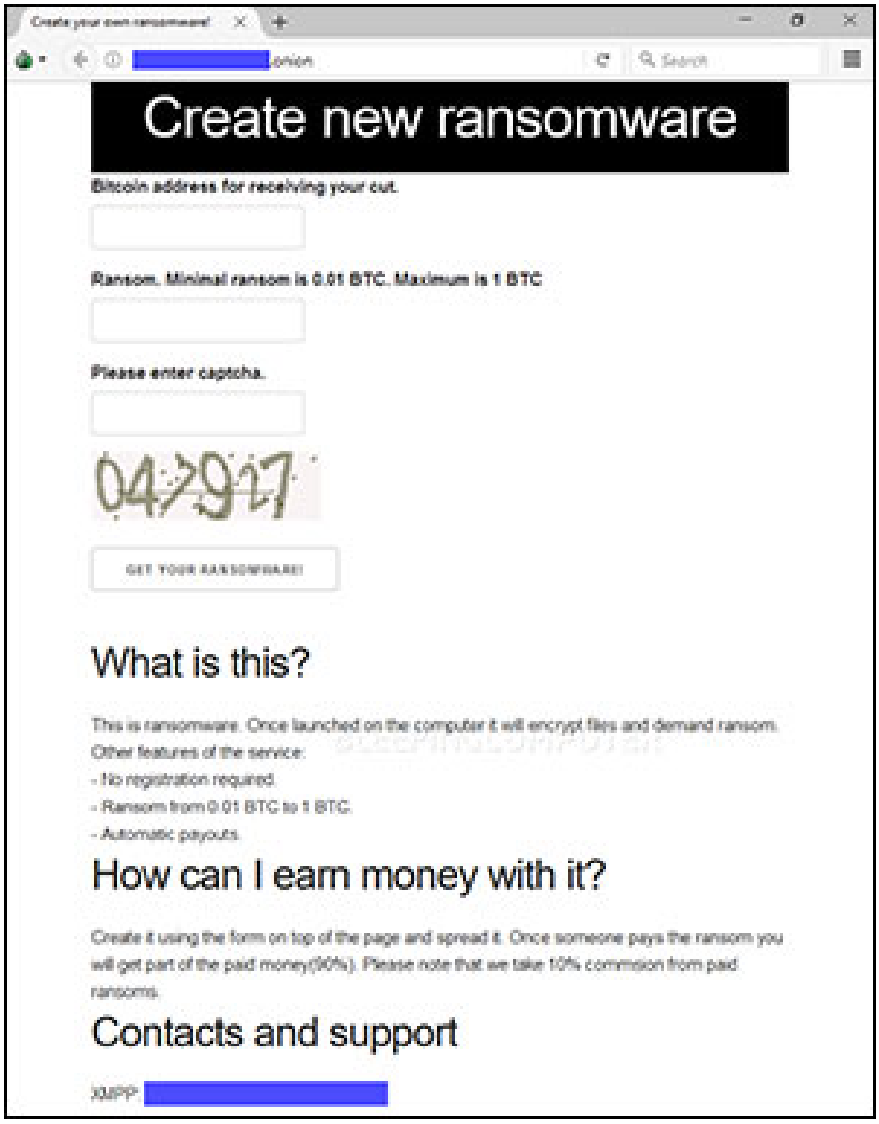
Over the past week, some network security researchers have discovered a new RaaS that allows anyone to create ransomware just by filling out a form with 3 fields and pressing a button to finish.

RaaS, short for Ransomware-as-a-Service (ransomware as a service) is a tool designed for anyone to use ransomware, almost without programming knowledge. . Compared to other detected Raas, this new tool requires very low skill.

Ransomware is created via a service written in Go. It is called Shifr due to the extension that adds encrypted files, but network security researcher G Data Karsten Hahn said that the initial analysis of the tool shows that Shifr might be relevant. to **Trojan.Encoder.6491,** the first ransomware was written in Go and was studied by Dr. security researchers. Web discovered last year.

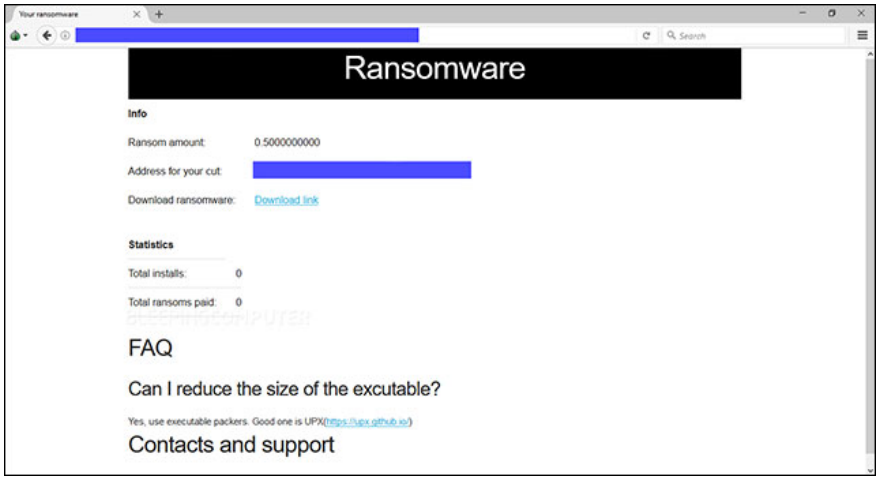
Shifr is a RaaS on Dark Web

To get this ransomware, you only need to visit the Dark Web site and a Bitcoin address. Customers only need to enter this Bitcoin address and the ransom they want Shifr to claim from the victim. After that, all you need to do is fill out the CAPTCHA and click the OK button.



Fill in the CAPTCHA and very simple steps to create ransomware

While other RAs will need you to pay a fee or verify customers to ensure only those with little skills (and not network security researchers) can use ransomware models, the service will provide Product level 'fully armed' in just a few easy steps.



Fill in some simple information to extort money with ransomware

Because of this simplicity and ease, VirusTotal has scanned a lot of Shifr in the past days, causing many antivirus software companies to pay attention and many of them now have the ability to detect this threat.

Shifr will only receive a 10% share

Besides being blatant, without stealth, this ransomware service is different from other RaSs in that it requires a very low share, making up for ransomware that lacks many features.

While Cerber RaaS service requires a 60% split, Shifr only needs 10%, obviously towards two groups of people: greedy people and very greedy people. With a 10% split, perhaps Shift will come with RAT or will steal information, money or tools from amateur ransomware spreaders. However, ransomware turned out to be nothing special. Shifr can also be a scam tool.

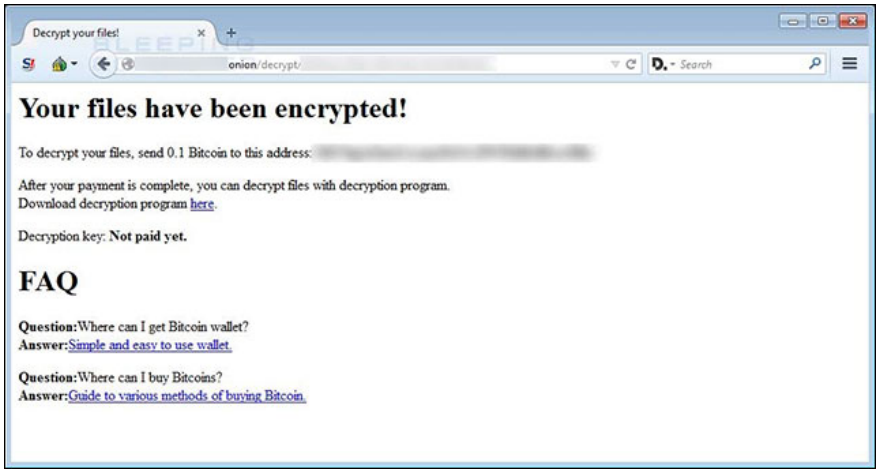
The victim after paying for the ransomware provider, will retain his share and pay the rest to the dispenser (owner of the Bitcoin address). Therefore, the provider can keep the money earned without paying the person who distributed the ransomware. Aiming at the greed of many people, Shifr can steal the ransom and not pay the dispenser.

Shifr is still in development

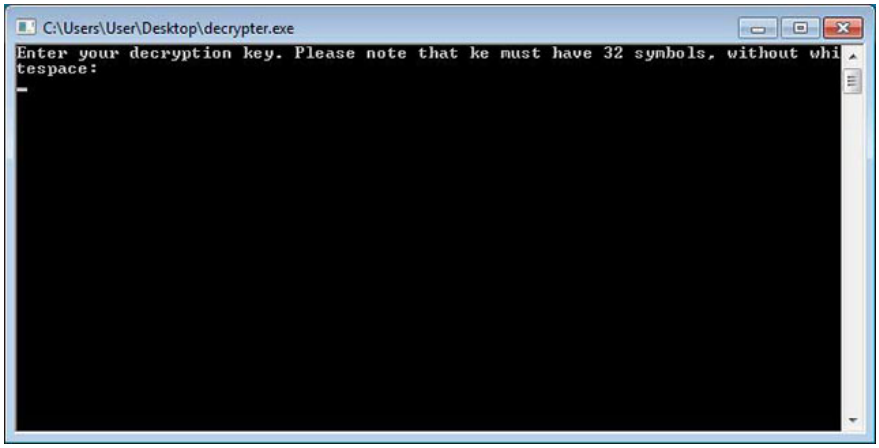
The simplicity of the ransomware provided by Shifr can be found in a very simple note that the victim receives, including only two lines with a link to the page to pay. In the test, the link did not even work and had to find the actual payment address based on other information.

Notify victims of encrypted files

The payment page is where the victim finds the Bitcoin address they will have to deposit with the link to decrypt their encrypted data. The original URL of this payment page is also the home page of RaaS, which means that the bad guys do not have enough equipment to separate their payments and RaaS into many different servers.



Payment instructions for decoding data



Enter the key paragraph after paying to unlock the file

RaaS appears more and more simple

Shifr is currently one of the simplest RaaS discovered in the past few years. The tendency to use RaSS seems to be moving from closed groups, secret forums to open websites for anyone to access. In a report published today, experts from Kaspersky Labs also noticed an increase in RaaS. The Kaspersky report also showed that the number of ransomwrae victims increased by 11.4% from 4/2016 to 3/2017, compared to the same period last year.

IOCs indicators

SHA256 hash

3c7d5bb131b98340ebe18f5d7f8ba289e8b91e017bf9d9ff8270e87a996d334d

Name of ransomware file

HOW_TO_DECRYPT_FILES.html

Ransomwrae's note notes

B?n t?p tin ?ã ???c xác ??nh.
To decrypt your files, follow instructions here.

Network requirements

http:/// [REDACTED] .onion / decrypt / f2f6d2aa-06e0-43f9-9ebd-853af768e29e
https: // [REDACTED] .onion.to / new_c /

The extension is encrypted

.shifr

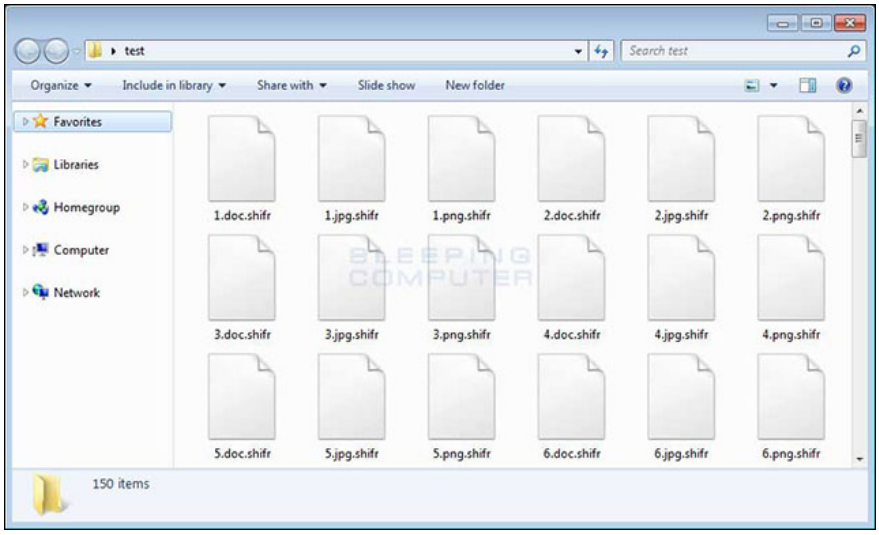


Image file is encrypted with the .shifr extension

The file extensions are targeted

* .accdb, *. arw, *. bay, *. cdr * .cr2, *. crw, *. csv, *. dcr, *. dng, *. doc, *. docx, *. dwg, *. dxf , *. erf, *. jpeg, *. jpg, *. kdc, *. mef, *. mrw, *. nef, *. nrw, *. orf, *. pdf, *. pef, *.

You finished reading the article "**New tool Shifr RaaS allows anyone to create ransomware easily**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.