Ransomware STOP started installing Trojans to steal victim passwords

In addition to encrypting files on the system, ransomware STOP strains have also started quietly installing the Azorult password stealing Trojan on the victim's computer to steal account information, electronic wallet, and file desktop ...

In addition to encrypting files on the system, ransomware STOP strains have also started quietly installing the Azorult password stealing Trojan on the victim's computer to steal account information, electronic wallet, and file desktop .

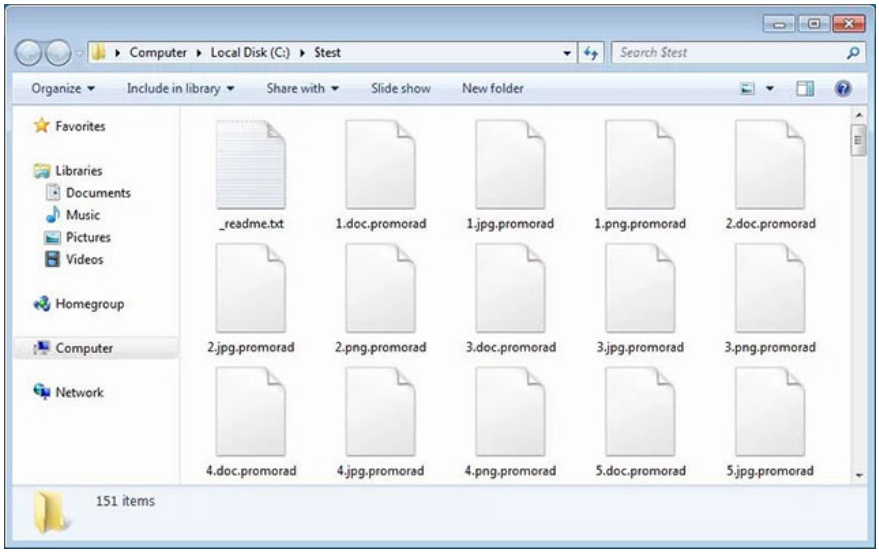
The Azorult Trojan is a type of malicious code that, when spread to a victim's computer, tries to steal user name and password information stored in the browser, as well as files on the victim's system. , electronic wallet, Steam login information, browser history, Skype message history, and many other valuable data. This information is then uploaded to a remote server under the control of the attacker.

1. Google has reported a zero-day vulnerability that has just appeared in Windows 7, Microsoft has not yet released a patch

When first presented with the DJVU variant of STOP ransomware, distributed by fake software vulnerabilities in January, security experts have noted that when malware is executed, it will be negative. silently download many other components, and they are used to perform various tasks on the victim's computer. These tasks include displaying a fake Windows Update screen, disabling Windows Defender, and blocking access to secure websites by adding items to Windows HOSTS files.

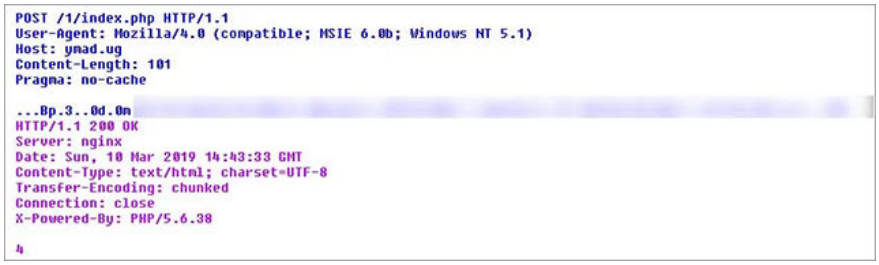
When ransomware researcher Michael Gillespie tested some of the recent variants of the malware, he found that the Any.Run installation indicates that one of the files downloaded by ransomware has generated traffic. Azorult malicious code access. Gillespie also revealed more to BleepingComputer that there are four different models that he found that show network traffic related to Azorult.

Experts at BleepingComputer then tried to download and install a sample of the STOP Promorad ransomware variant to see if Azorult was installed as Michael Gillespie said. And indeed, when ransomware spreads on the BleepingComputer system, it proceeded to download the files listed in the IOC below and encrypt the computer. In this specific variant, when the files are encrypted, it will append the .promorad extension to those files and create a ransom note named _readme.txt, as shown in the image below.



1. There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

The Promorad ransomware variant model that researchers at BleepingComputer also automatically downloaded a file named 5.exe and silently executed it. When implemented, the program will generate identical network traffic with the communications of the command and control server known to the Azorult information stealing Trojan.



Furthermore, after scanning with VirusTotal, many security vendors have discovered essentially, this file is a password stealing Trojan.

After becoming a victim of this ransomware, determining whether your password and documents have been stolen is an important issue that users need to consider.

The victim has been infected with the STOP ransomware variant and should immediately change the password of any online account that is being used and saved on the system, with special attention being paid to the accounts stored in the program. Browser. In addition, Victims should also change passwords stored in software such as Skype, Steam, Telegram and FTP Client. The last thing to do is check all the files that are being stored on the Windows desktop to determine if your personal information is in the hands of the attacker.

1. Supercomputers can completely detect cyber threats

In the past, ransomware STOP has not stopped "evolving" and became a popular malicious code with a variety of variants, and it is currently impossible to determine how long they have installed Azorult. Therefore, to ensure safety, all STOP victims should immediately take the above remedies.

The list of extensions of known ransomware STOP strains includes:

```
.blower
.djvu
.infowait
.promok
.promorad2
.promos
.promoz
.puma
.rumba
.ash
```

If you have any concerns or questions regarding this ransomware software, you can post your questions in the dedicated Help & Help page about BleepingComputer STOP ransomware related issues here. .

You finished reading the article "**Ransomware STOP started installing Trojans to steal victim passwords**" 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.