The Velso Ransomware Being Manually Installed by Attackers

bleepingcomputer.com/news/security/the-velso-ransomware-being-manually-installed-by-attackers

By
Lawrence Abrams

- January 26, 2018
- 12:55 PM
- 0

A new ransomware is actively infecting victims called the Velso Ransomware. This ransomware appends the **.velso** extension to encrypted files and then drops a ransom note that contains an email address that a victim can use to contact the developer.

In this article I will provide a brief summary of what we know about the velso ransomware and how you can protect yourself from it. You can also discuss or receive support for the Velso Ransomware in our dedicated Velso Ransomware Help & Support Topic.

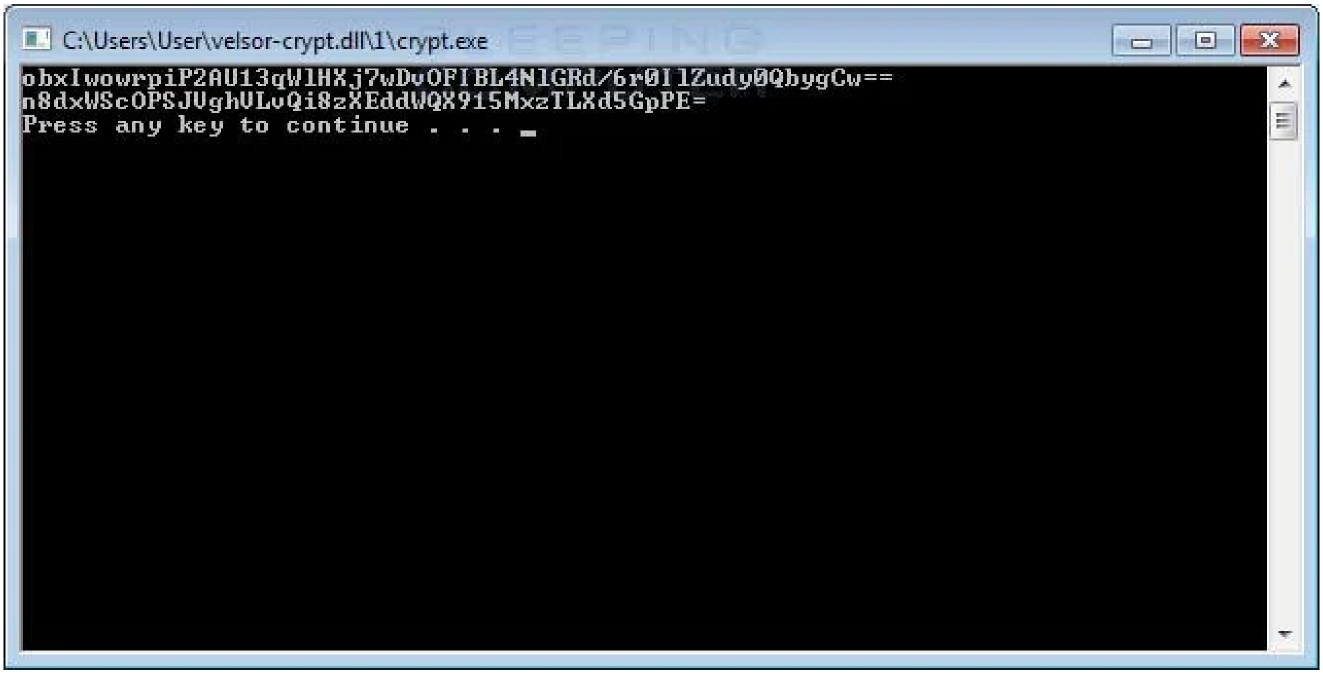
What we know about the Velso Ransomware

The Velso Ransomware was first discovered by Michael Gillespie when saw a submission to his ID-Ransomware site. After tweeting about the sample, another researcher named Martin Stopka was able to find a sample of the infection.

> https://t.co/L1zrLcUbOC
>
> — Martin Stopka (@stopka_martin) January 17, 2018

While it is not 100% confirmed, it appears that the Velso Ransomware is installed manually by an attacker hacking into a victim's computer via remote desktop services. The attacker then manually executes the ransomware file. This causes it to display the victim's ID and then the decryption key while it pauses waiting for the attacker to press a key on the keyboard.

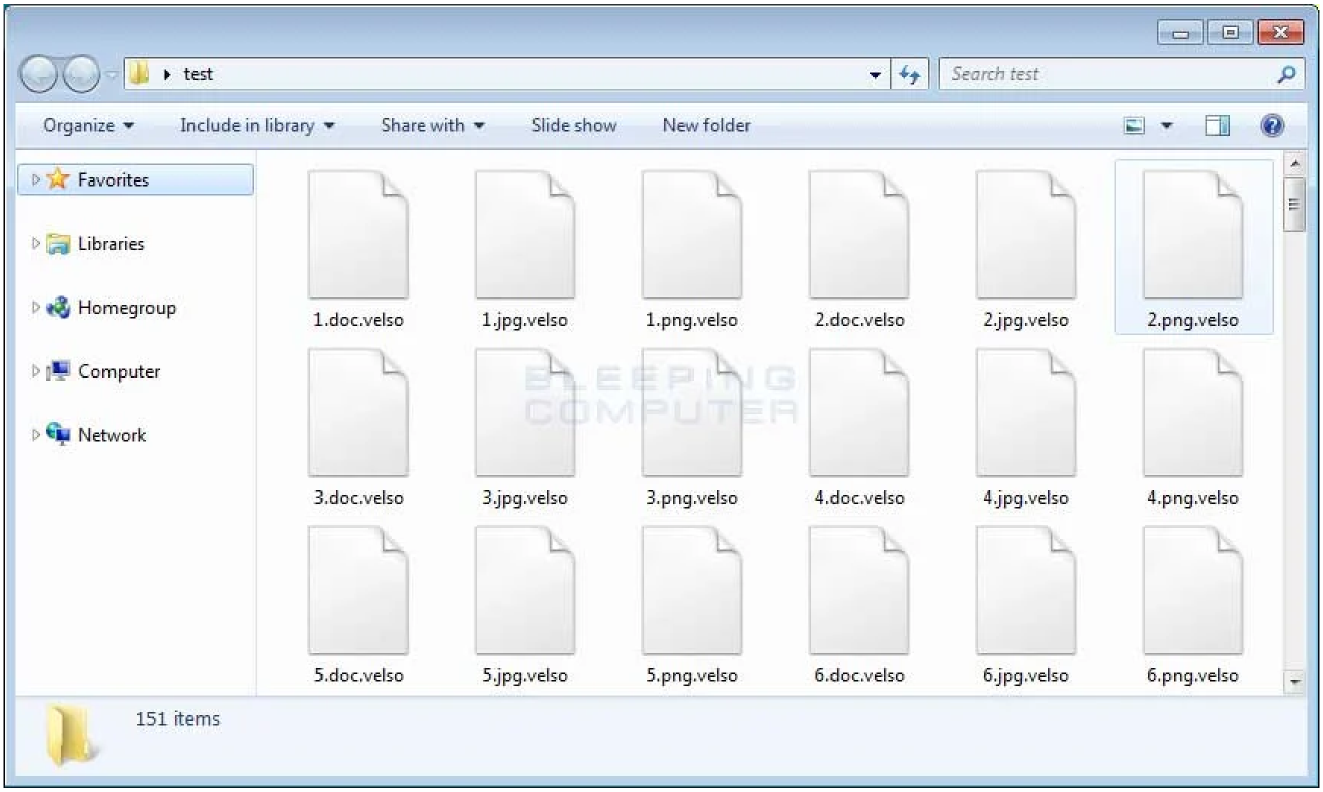
Once the attacker has finished copying the two strings, they can press any key and start the process of encrypting the computer. You can see below what the ransomware looks like when it was executed by BleepingComputer.



```
obxIwowrpiP2AU13qWlHXj7wDvOFIBL4N1GRd/6r0IlZudy0QbygCw==
n8dxWScOPSJUghVLvQi8zXEddWQX915MxzTLXd5GpPE=
Press any key to continue . . . _
```

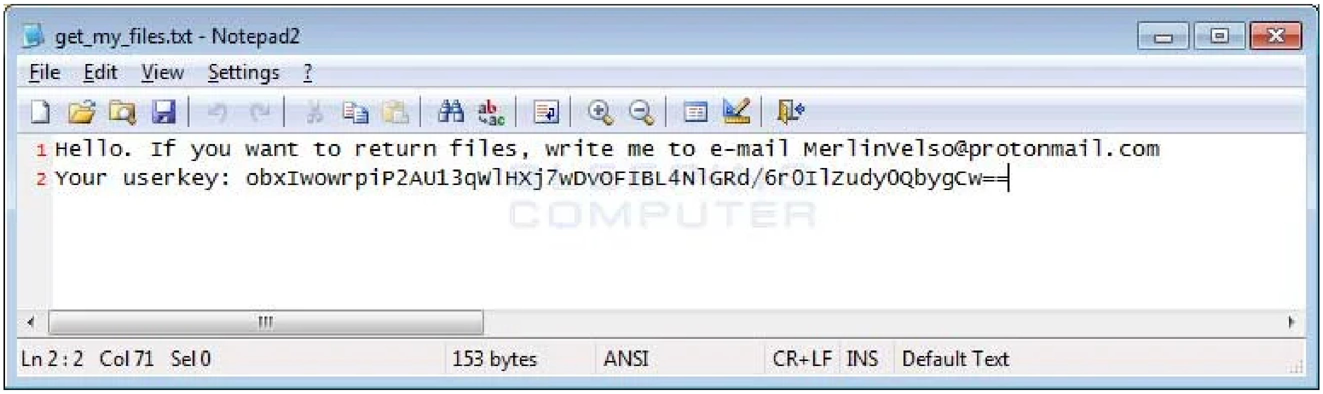
Velso Ransomware

When encrypting files, it will modify the filename by appending the .velso extension to the encrypted file's name. For example, a file named test.jpg would be encrypted and renamed to test.jpg.velso.



Folder of Encrypted Velso Files

A ransom note will also be created in every folder that a file is encrypted. This ransom note is named **get_my_files.txt** and contains an email address that a victim can contact for payment instructions and the victim's unique ID. The current email address is MerlinVelso@protonmail.com.



```
Hello. If you want to return files, write me to e-mail Merlinvelso@protonmail.com
Your userkey: obxIwowrpiP2AU13qWlHXj7wDVOFIBL4NlGRd/6rOIlzudyOQbygCw==
```

Velso Ransom Note

The get_my_files.txt will be copied in the Windows Startup folder so that it is automatically displayed when a user logs into the computer.

Unfortunately, at this time there are no known weaknesses that could allow a victim to recover their files for free.

How to protect yourself from the Velso Ransomware

To protect yourself from the Velso Ransomware, it is particularly important that you do not have any computers running remote desktop services connected directly to the Internet. Instead place computers running remote desktop behind VPNs so that they are only accessible to those who have VPN accounts on your network.

In order to protect yourself from ransomware in general, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,

- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

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

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

Server Hashes:

```
SHA256: 4c8cf7ce3836edceb540edeccae97ef182331f6ed93e678d2e33105d01e809bf
```

Filenames associated with the Server Cryptomix Variant:

```
get_my_files.txt
```

Server Ransom Note Text:

```
Hello. If you want to return files, write me to e-mail MerlinVelso@protonmail.com
Your userkey: obxIwowrpiP2AU13qWlHXj7wDvOFIBL4NlGRd/6r0IlZudy0QbygCw==
```

Emails Associated with the Server Ransomware:

```
MerlinVelso@protonmail.com
```

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.