Ransom.Megacortex | Malwarebytes Labs

Archived: 2026-04-06 00:56:56 UTC

Short bio

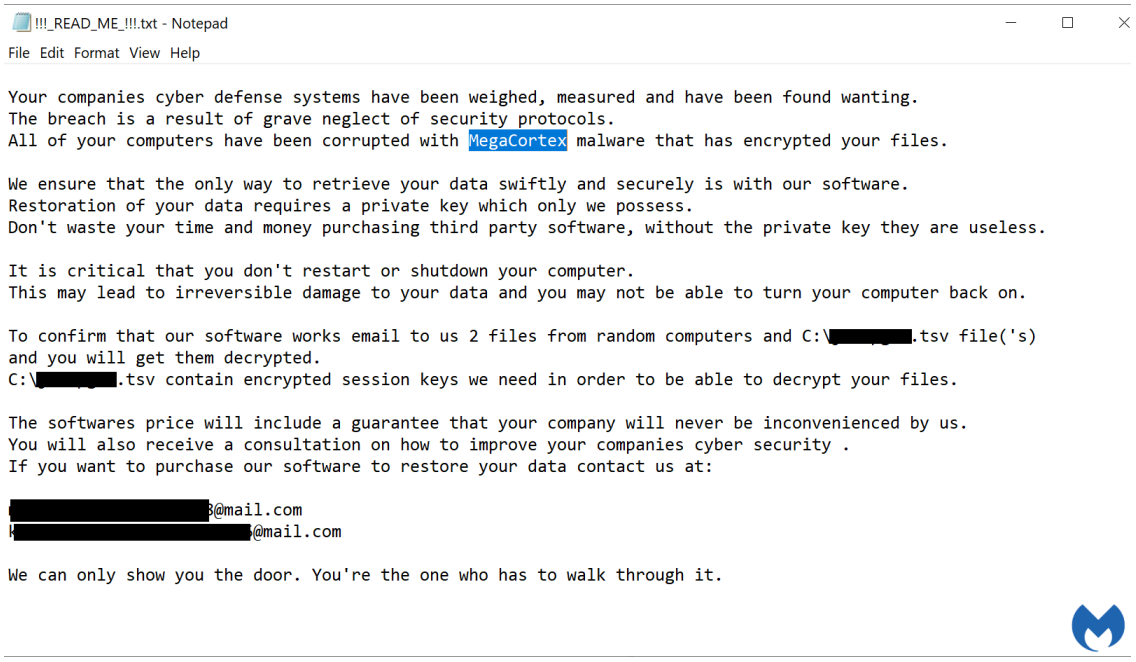
Ransom.Megacortex is Malwarebytes' detection name for a small family of ransomware that is used in targeted attacks on enterprises.

Symptoms

Ransom.Megacortex tries to stop several processes that belong to security software.

Ransom.MegaCortex adds the extension .aes128ctr to the encrypted files.

When the encryption routine has completed it will show a ransom note which mentions a tsv file in the root directory and two email addresses.

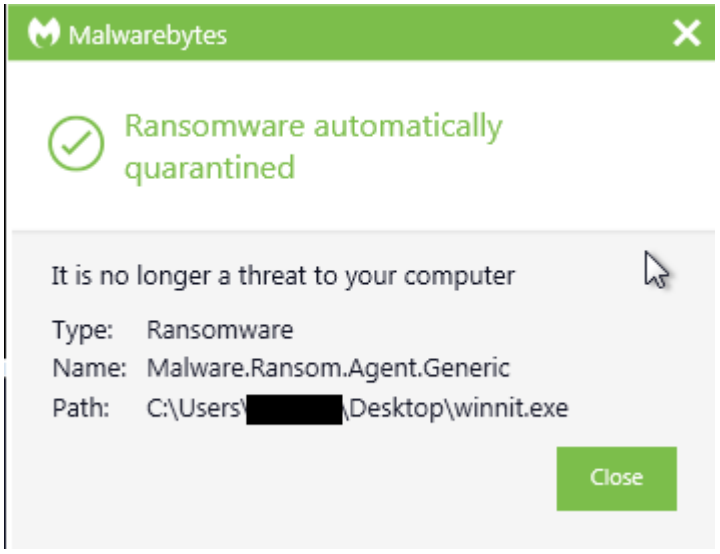


Type and source of infection

Ransom.Megacortex is ransomware. Ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. Ransom.Megacortex is introduced on enterprise networks by use of stolen or leaked administrative credentials. There are also some reports of the threat actors using Trojan downloaders that are spread through instant messaging networks. These are spread and then used to download and install the ransomware.

Protection

Malwarebytes blocks Ransom.Megacortex



Business remediation

Malwarebytes can detect and remove Ransom.Megacortex on business machines without further user interaction. To remove Ransom.Megacortex using Malwarebytes business products, follow the instructions below.

How to remove Ransom.Megacortex with Malwarebytes Endpoint Protection

1. Go to the Malwarebytes Cloud console.
2. To allow you to invoke a scan while the machine is off the network, go to **Settings** > **Policies** > **your policy** > **General**.
3. Under **Endpoint Interface Options**, turn ON:
    1. Show Malwarebytes icon in notification area
    2. Allow users to run a Threat Scan (all threats will be quarantined automatically)
4. Once the endpoint has been updated with the latest policy changes: take the client off the network

If you have infected machines that are not registered endpoints in Malwarebytes Endpoint Protection, you can remove Ransom.Megacortex with our Breach Remediation tool (MBBR).

1. Log into your My Account page and copy your license key. The key is needed to activate MBBR tool.
2. Open your Cloud console.
3. From a clean and safe machine, go to **Endpoints > Add > Malwarebytes Breach Remediation.** This will download the MBBR zip package.
4. Unzip the package.
5. Access a Windows command line prompt and issue the following commands: mbbr register –key: mbbr update **Note**: You must substitute your license key for .
6. Copy the MBBR folder to a flash drive.
7. From an infected, offline machine, copy the MBBR folder from the flash drive.
8. Start a scan using the following command: mbbr scan –full –ark –remove –noreboot
9. Refer to the Malwarebytes Breach Remediation Windows Administrator Guide for all supported scanning commands.

Consumer remediation

Malwarebytes can detect and remove Ransom.Megacortex without further user interaction.

1. Please download Malwarebytes to your desktop.
2. Double-click **MBSetup.exe** and follow the prompts to install the program.
3. When your **Malwarebytes for Windows** installation completes, the program opens to the Welcome to Malwarebytes screen.
4. Click on the **Get started** button.
5. Click **Scan** to start a **Threat Scan**.
6. Click **Quarantine** to remove the found threats.
7. Reboot the system if prompted to complete the removal process.

Take note, however, that removing this ransomware does not decrypt your files. You can only get your files back from backups you made before the infection happened.

IOCs

IP address:

89.105.198.28

Filename:

winnit.exe

File hashes: 5e973e6096174590ed667c4f5e4dc3e4 c8d78aeaa3d0daefa3b916457b529bfe ea153f0de16bbdd1abd0a669cb126007 e0c75ef549db413ae5acde363977584a **Ransom note:** !!!_READ_ME_!!!.txt **Key file:** c:********.tsv (********= 8 random characters)

Source: https://blog.malwarebytes.com/detections/ransom-megacortex/