Ransom.GlobeImposter

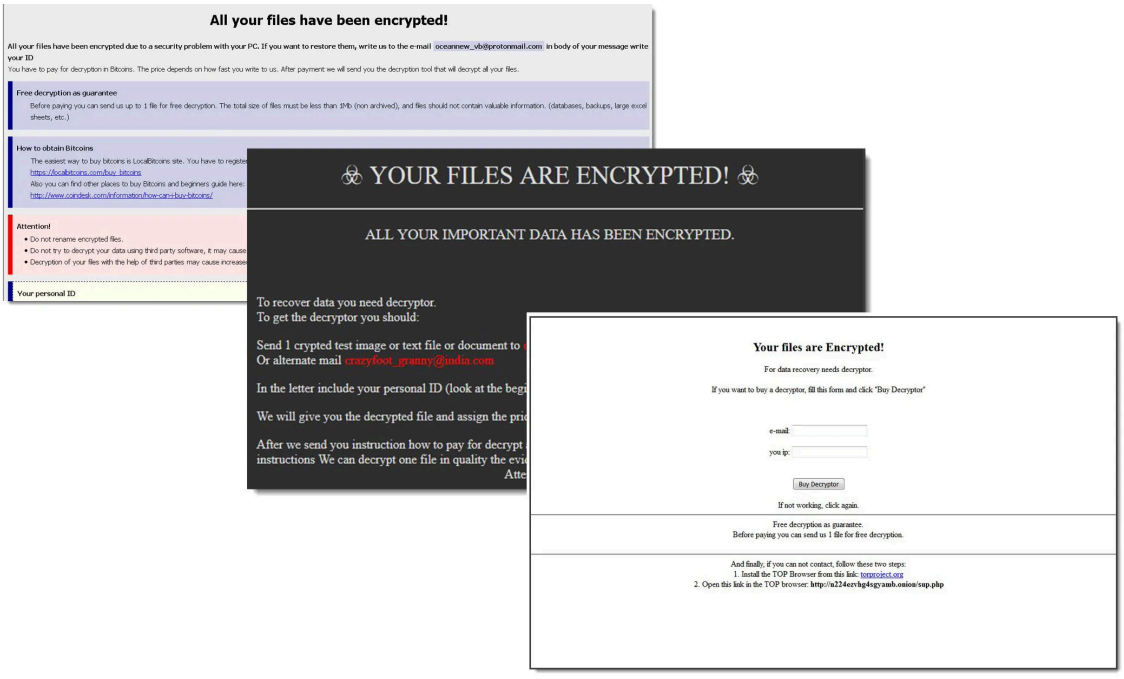
Archived: 2026-04-05 19:58:06 UTC

Short bio

Ransom.GlobeImposter is a ransomware application that will encrypt files on a victim machine and demand payment to retrieve the information. Ransom.GlobeImposter is also known as Fake Globe due to how the software mimics the Globe ransomware family . Ransom.GlobeImposter may be distributed through a malicious spam campaign, recognizable only with their lack of message content and an attached ZIP file. This type of spam is called a “blank slate.” Ransom.GlobeImposter is also distributed via exploits and malicious advertising, fake updates, and repacked infected installers.

Symptoms

Ransom.GlobeImposter may run silently in the background during the encryption phase and not provide any indication of infection to the user. Ransom.GlobeImposter may prevent the execution of Antivirus programs and other Microsoft Windows security features and may prevent system restoration as a means to solicit payment. Ransom.Cryptomix may display a warning after successful encryption of the victim machine.



Type and source of infection

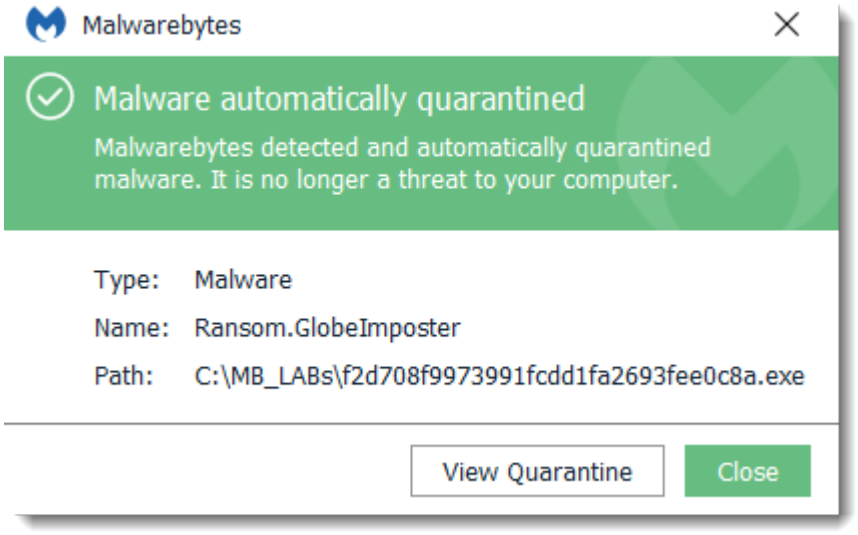
Ransom.GlobeImposter may be distributed using various methods. This software may be packaged with free online software, or could be disguised as a harmless program and distributed by email. Alternatively, this software may be installed by websites using software vulnerabilities. Infections that occur in this manner are usually silent and happen without user knowledge or consent.

Aftermath

Systems affected by ransomware are rendered unusable due to files that are typically used for regular operations being encrypted.Affected users who choose to pay the threat actors behind ransomware campaigns in exchange for access to data may find that they don't get their files back. There is also no sure way to know that threat actors will honor their end of the deal after paying the ransom.Affected users who chose to pay the threat actors may also find themselves likely targets for future ransomware campaigns.Data held hostage that wasn't given back to users or deleted after the ransom has been paid can be used by threat actors either to (a) sell on the black market or (b) create a profile of the user they can use for fraud.

Protection

Malwarebytes protects users from the installation of Ransom.GlobeImposter.



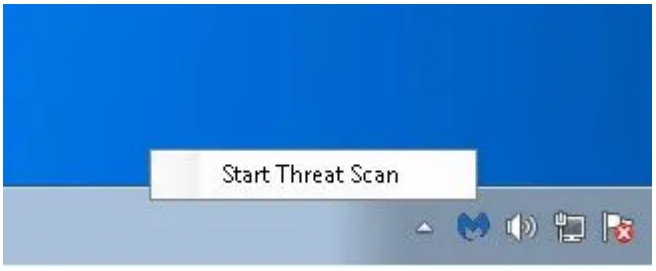
Business remediation

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

How to remove Ransom.GlobeImposter 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. Temporarily enable Anti-Rootkit scanning for all invoked threat scans.Go to **Settings**> **Policies**> **your policy**> **Endpoint Protection**> **Scan Options**
5. Set **Scan Rootkits**to ON.
6. Once the endpoint has been updated with the latest policy changes:
    1. Take the client off the network
    2. From the system tray icon, run an Anti-Rootkit threat scan.



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

1. Log into your My Account pageand 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 Guidefor all supported scanning commands.

Remediation

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

1. Please download Malwarebytesto 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.

Traces/IOCs

Ransom file extensions

.402	.fuck	.scorp
.4035	.goro	.sea
.4090	.gotham	.skunk
.4091	.granny	.Trump
.452	.happ	.txt
.707	.Ipcrestore	.UNLIS
.725	.keepcalm	.vdul
.726	.LIN	.wallet
.911	.MAKB	.write_me_[email]
.f41o1	.medal	.write_on_email
.2cXpCihgsVxB3	.mtk118	.write_us_on_email
.3ncrypt3d	.needdecrypt	.YAYA
.au1crypt	.needkeys	.zuzya
.BONUM	.NIGGA	..doc
.BRT92	.nWcrypt	.encencenc
.BUSH	.paycyka	.{email@aol.com}BIT
.C8B089F	.pizdec	.[email@cock.li].arena
.CHAK	.pscrypt	.lock
.clinTON	.ReaGAN	.Nutella
.crypt	.rumblegoodboy	.waiting4keys
.FIX	.s1crypt	.FREEMAN