Ransomware dev releases Egregor, Maze master decryption keys

bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/

Lawrence Abrams

By
Lawrence Abrams

- February 9, 2022
- 10:26 AM
- 4

The master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released last night on the BleepingComputer forums by the alleged malware developer.

The Maze ransomware began operating in May 2019 and quickly rose to fame as they were responsible for the use of data theft and double-extortion tactics now used by many ransomware operations.

After Maze announced its shutdown in October 2020, they rebranded in September as Egregor, who later disappeared after members were arrested in Ukraine.

The Sekhmet operation was somewhat of an outlier as it launched in March 2020, while Maze was still active.

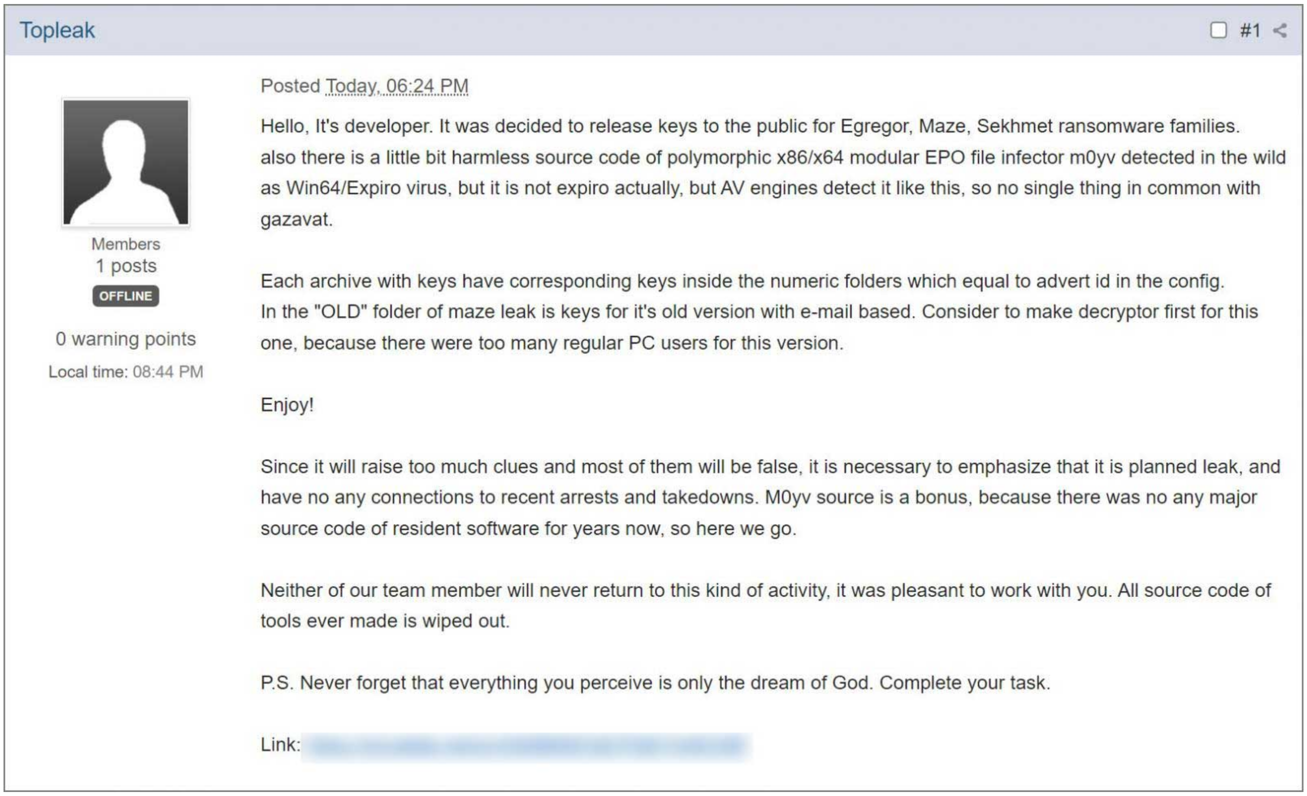
Master decryption keys released

Fast forward 14 months later, and the decryption keys for these operations have now been leaked in the BleepingComputer forums by a user named 'Topleak' who claims to be the developer for all three operations.

The poster said that this was a planned leak and is not related to recent law enforcement operations that have led to the seizing of servers and the arrests of ransomware affiliates.

"Since it will raise too much clues and most of them will be false, it is necessary to emphasize that it is planned leak, and have no any connections to recent arrests and takedowns," explained the alleged ransomware developer.

They further stated that none of their team members will ever return to ransomware and that they destroyed all of the source code for their ransomware.



Topleak □ #1

Members
1 posts
OFFLINE
0 warning points
Local time: 08:44 PM

Posted Today, 06:24 PM

Hello, It's developer. It was decided to release keys to the public for Egregor, Maze, Sekhmet ransomware families. also there is a little bit harmless source code of polymorphic x86/x64 modular EPO file infector m0yv detected in the wild as Win64/Expiro virus, but it is not expiro actually, but AV engines detect it like this, so no single thing in common with gazavat.

Each archive with keys have corresponding keys inside the numeric folders which equal to advert id in the config.
In the "OLD" folder of maze leak is keys for it's old version with e-mail based. Consider to make decryptor first for this one, because there were too many regular PC users for this version.

Enjoy!

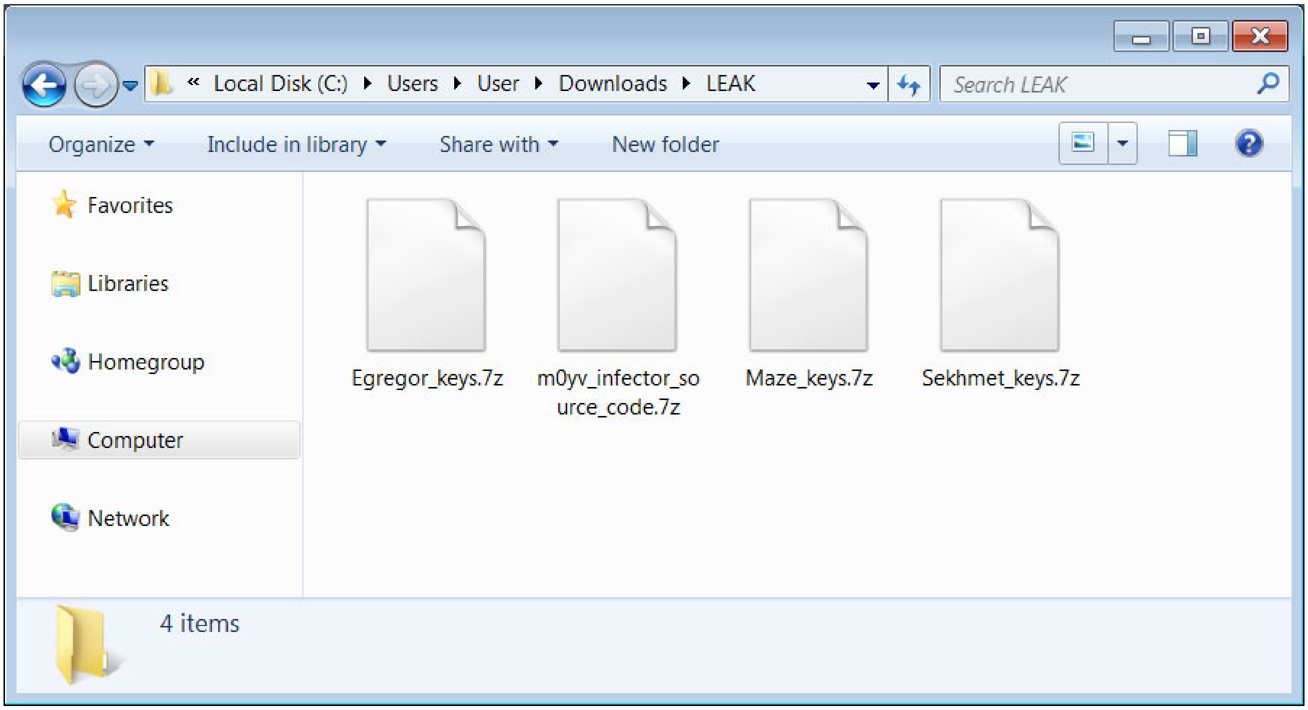
Since it will raise too much clues and most of them will be false, it is necessary to emphasize that it is planned leak, and have no any connections to recent arrests and takedowns. M0yv source is a bonus, because there was no any major source code of resident software for years now, so here we go.

Neither of our team member will never return to this kind of activity, it was pleasant to work with you. All source code of tools ever made is wiped out.

P.S. Never forget that everything you perceive is only the dream of God. Complete your task.

Link: [redacted]

Forum post leaking Maze, Egregor, and Sekhmet decryption keys
Source: BleepingComputer
The post includes a download link for a 7zip file with four archives containing the Maze, Egregor, and Sekhmet decryption keys, and the source code for a 'M0yv' malware used by the ransomware gang.



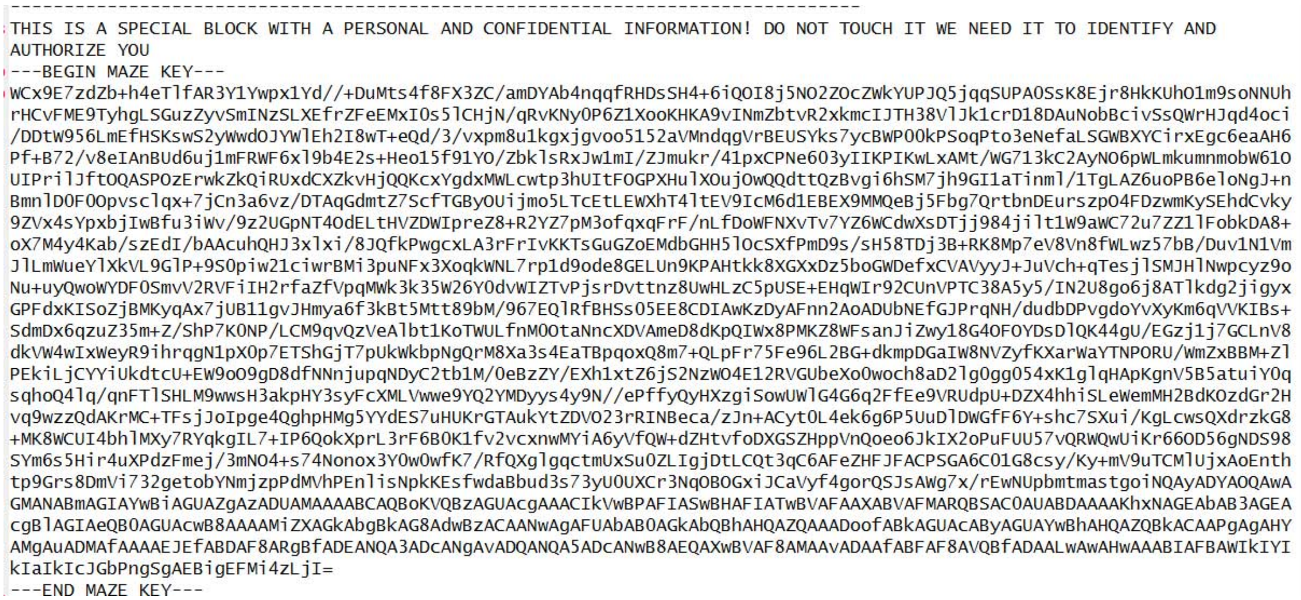
Archive containing the leaked decryption keys
Source: BleepingComputer
Each of these archives contains the public master encryption key and the private master decryption key associated with a specific "advert", or affiliate of the ransomware operation.

In total, the following are the number of RSA-2048 master decryption keys released per ransomware operation:

- **Maze:** 9 master decryption keys for the original malware that targeted non-corporate users.
- **Maze:** 30 master decryption keys.
- **Egregor:** 19 master decryption keys.
- **Sekhmet**: 1 master decryption key.

Emsisoft's Michael Gillespie and Fabian Wosar has reviewed the decryption keys and confirmed to BleepingComputer that they are legitimate and can be used to decrypt files encrypted by the three ransomware families.

Gillespie told us that the keys are used to decrypt a victim's encrypted keys that are embedded in a ransom note.



```
-------------------------------------------------------------------------------
THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO NOT TOUCH IT WE NEED IT TO IDENTIFY AND
AUTHORIZE YOU
---BEGIN MAZE KEY---
```

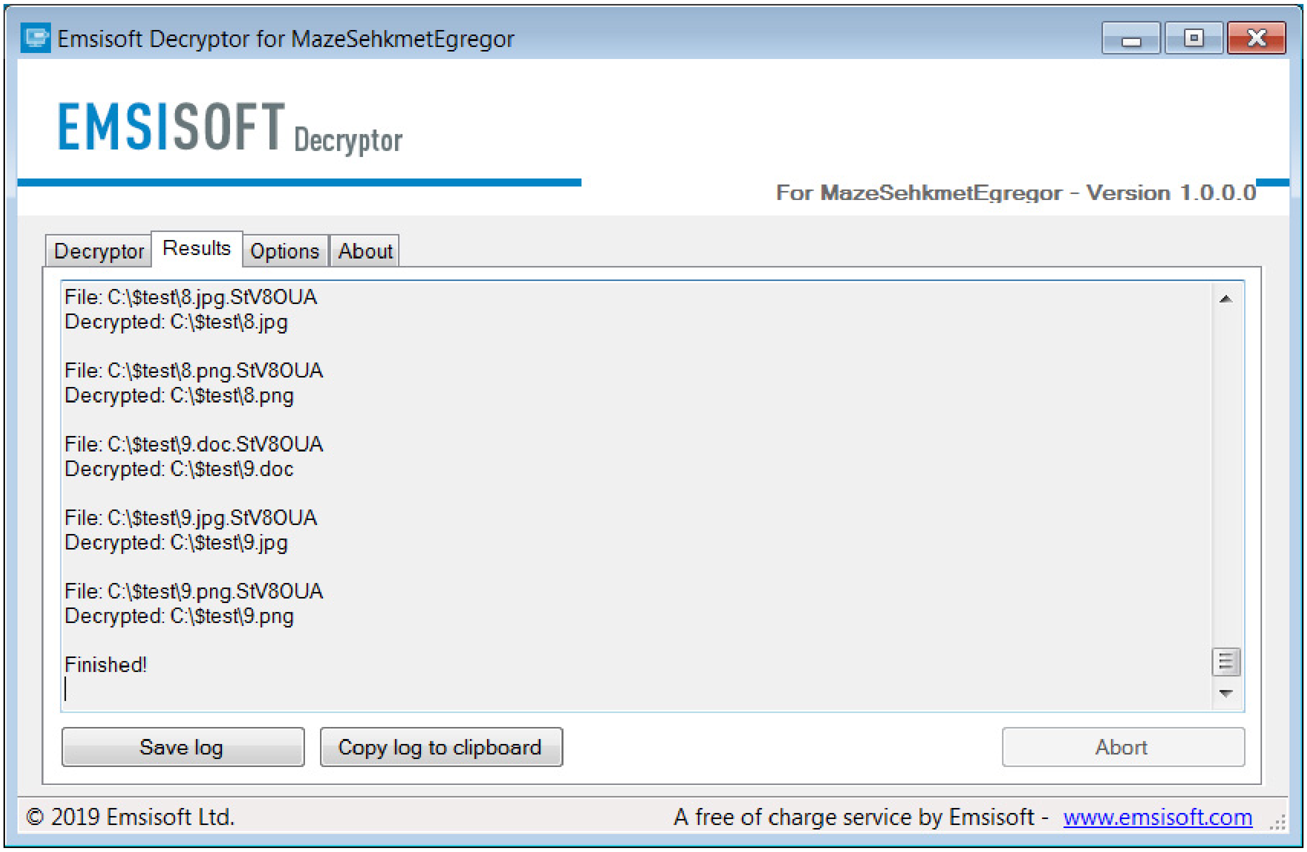
```
WCx9E7zdZb+h4eTlfAR3Y1Ywpx1Yd//+DuMts4f8FX3ZC/amDYAb4nqqfRHDsSH4+6iQOI8j5NO2ZOcZWkYUPJQ5jqqSUPA0SsK8Ejr8HkKUhO1m9soNNUh
rHCvFME9TyhgLSGuzZyvSmINzSLXEfrZFeEMxIOs5lCHjN/qRvKNyOP6Z1XooKHKA9vINmZbtvR2xkmcIJTH38VlJk1crD18DAuNobBcivSsQWrHJqd4oci
/DDtW956LmEfHSKswS2yWwdOJYWlEh2I8wT+eQd/3/vxpm8u1kgxjgvoo5152aVMndqgVrBEUSYks7ycBWPO0kPSoqPto3eNefaLSGWBXYCirxEgc6eaAH6
Pf+B72/v8eIAnBUd6uj1mFRWF6xl9b4E2s+Heo15f91YO/ZbklsRxJw1mI/ZJmukr/41pxCPNe603yIIKPIKwLxAMt/WG713kC2AyNO6pWLmkumnmobW61O
UIPrilJftOQASPOzErwkZkQiRUxdCXZkvHjQQKcxYgdxMWLcwtp3hUItFOGPXHulXOujOwQQdttQzBvgi6hSM7jh9GI1aTinml/1TgLAZ6uoPB6eloNgJ+n
BmnlDOFOOpvsclqx+7jCn3a6vz/DTAqGdmtZ7ScfTGByOUijmo5LTcEtLEWXhT4ltEV9IcM6d1EBEX9MMQeBj5Fbg7QrtbnDEurszpO4FDzwmKySEhdCvky
9ZVx4sYpxbjIwBfu3iWv/9z2UGpNT4OdELtHVZDWIpreZ8+R2YZ7pM3ofqxqFrF/nLfDoWFNXvTv7YZ6WCdwXsDTjj984jilt1W9aWC72u7ZZ1lFobkDA8+
oX7M4y4Kab/szEdI/bAAcuhQHJ3xlxi/8JQfkPwgcxLA3rFrIvKKTsGuGZoEMdbGHH5lOcSXfPmD9s/sH58TDj3B+RK8Mp7eV8Vn8fWLwz57bB/Duv1N1Vm
JlLmWueYlXkVL9GlP+9SOpiw21ciwrBMi3puNFx3XoqkWNL7rp1d9ode8GELUn9KPAHtkk8XGXxDz5boGWDefxCVAVyyJ+JuVch+qTesjlSMJHlNwpcyz9o
Nu+uyQwoWYDFOSmvV2RVFiIH2rfaZfVpqMWk3k35W26YOdvWIZTvPjsrDvttnz8UwHLzC5pUSE+EHqWIr92CUnVPTC38A5y5/IN2U8go6j8ATlkdg2jigyx
GPFdxKISoZjBMKyqAx7jUB11gvJHmya6f3kBt5Mtt89bM/967EQlRfBHSs05EE8CDIAwKzDyAFnn2AoADUbNEfGJPrqNH/dudbDPvgdoYvXyKm6qVVKIBs+
SdmDx6qzuZ35m+Z/ShP7K0NP/LCM9qvQzVeAlbt1KoTWULfnM0OtaNncXDVAmeD8dKpQIWx8PMKZ8WFsanJiZwy18G4OFOYDsDlQK44gU/EGzj1j7GCLnV8
dkVW4wIxWeyR9ihrqgN1pXOp7ETShGjT7pUkWkbpNgQrM8Xa3s4EaTBpqoxQ8m7+QLpFr75Fe96L2BG+dkmpDGaIW8NVZyfKXarWaYTNPORU/WmZxBBM+Zl
PEkiLjCYYiUkdtcU+EW9oO9gD8dfNNnjupqNDyC2tb1M/0eBzZY/EXh1xtZ6jS2NzWO4E12RVGUbeXo0woch8aD2lg0gg054xK1glqHApKgnV5B5atuiY0q
sqhoQ4lq/qnFTlSHLM9wwsH3akpHY3syFcXMLVwwe9YQ2YMDyys4y9N//ePffyQyHXzgiSowUWlG4G6q2FfEe9VRUdpU+DZX4hhiSLeWemMH2BdKOzdGr2H
vq9wzzQdAKrMC+TFsjJoIpge4QghpHMg5YYdES7uHUKrGTAukYtZDVO23rRINBeca/zJn+ACyt0L4ek6g6P5UuDlDWGfF6Y+shc7SXui/KgLcwsQXdrzkG8
+MK8WCUI4bhlMXy7RYqkgIL7+IP6QokXprL3rF6BOK1fv2vcxnwMYiA6yVfQW+dZHtvfoDXGSZHppVnQoeo6JkIX2oPuFUU57vQRWQwUiKr66OD56gNDS98
SYm6s5Hir4uXPdzFmej/3mNO4+s74Nonox3YOw0wfK7/RfQXglgqctmUxSu0ZLIgjDtLCQt3qC6AFeZHFJFACPSGA6C01G8csy/Ky+mV9uTCMlUjxAoEnth
tp9Grs8DmVi732getobYNmjzpPdMVhPEnlisNpkKEsfwdaBbud3s73yU0UXCr3NqOBOGxiJCaVyf4gorQSJsAWg7x/rEwNUpbmtmastgoiNQAyADYAOQAwA
GMANABmAGIAYwBiAGUAZgAzADUAMAAAABCAQBoKVQBzAGUAcgAAACIkVwBPAFIASwBHAFIATwBVAFAAXABVAFMARQBSAC0AUABDAAAAKhxNAGEAbAB3AGEA
cgBlAGIAeQB0AGUAcwB8AAAAMiZXAGkAbgBkAG8AdwBzACAANwAgAFUAbAB0AGkAbQBhAHQAZQAAADoofABkAGUAcAByAGUAYwBhAHQAZQBkACAAPgAgAHY
AMgAuADMAfAAAAEJEfABDAF8ARgBfADEANQA3ADcANgAvADQANQA5ADcANwB8AEQAXwBVAF8AMAAvADAAfABFAF8AVQBfADAALwAwAHwAAABIAFBAWIkIYI
kIaIkIcJGbPngSgAEBigEFMi4zLjI=
```

```
---END MAZE KEY---
```

Encrypted key in Maze ransom note

Source: BleepingComputer

Emsisoft has released a decryptor to allow any Maze, Egregor, and Sekhmet victims who have been waiting to recover their files for free.



Emsisoft Decryptor for MazeSehkmetEgregor
EMSISOFT Decryptor
For MazeSehkmetEgregor - Version 1.0.0.0
Decryptor
Results
Options
About
Save log
Copy log to clipboard
Abort
© 2019 Emsisoft Ltd.
A free of charge service by Emsisoft - www.emsisoft.com

```
File: C:\$test\8.jpg.StV8OUA
Decrypted: C:\$test\8.jpg

File: C:\$test\8.png.StV8OUA
Decrypted: C:\$test\8.png

File: C:\$test\9.doc.StV8OUA
Decrypted: C:\$test\9.doc

File: C:\$test\9.jpg.StV8OUA
Decrypted: C:\$test\9.jpg

File: C:\$test\9.png.StV8OUA
Decrypted: C:\$test\9.png

Finished!
```

Emsisoft decryptor for Maze, Egregor, and Sekhmet

To use the decryptor, victims will need ransom note created during the attack as it contains the encrypted decryption key.

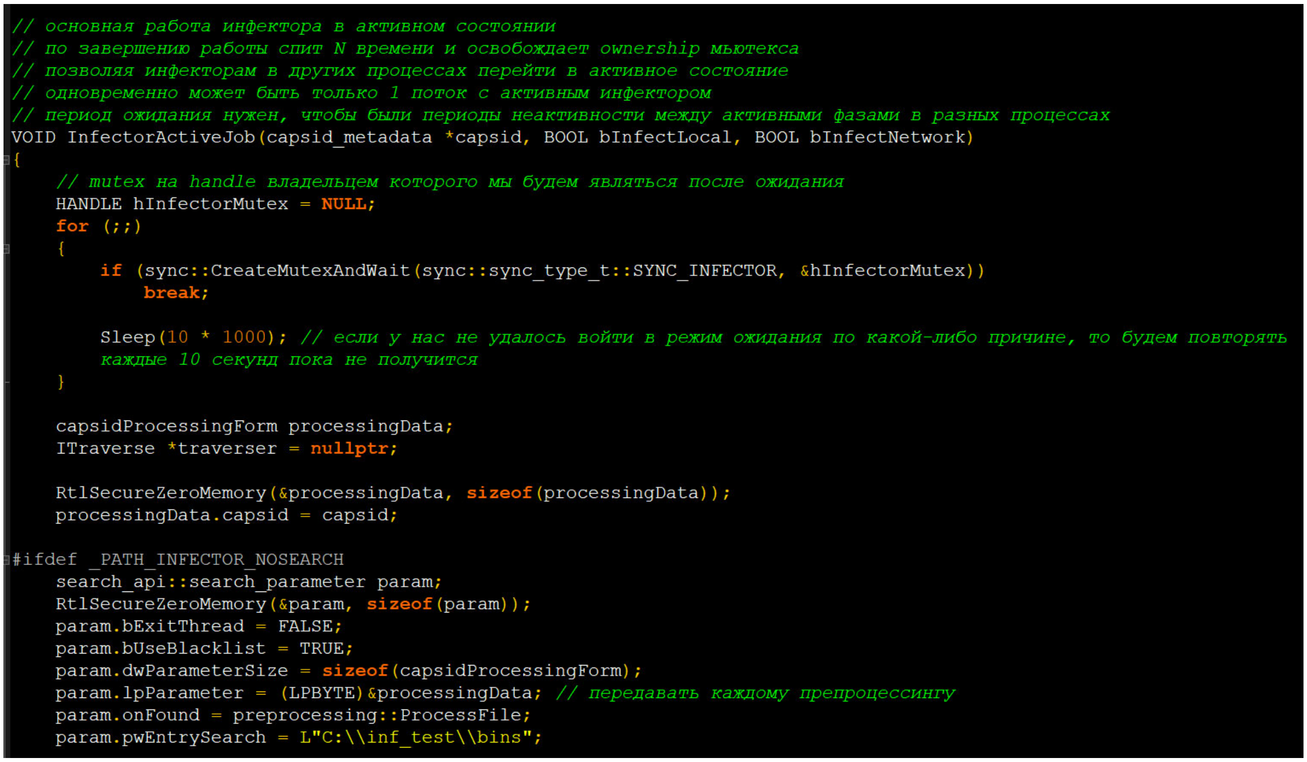
Bonus M0yv malware source code

The archive also includes the source code for the M0yv 'modular x86/x64 file infector' developed by the Maze ransomware operation and used previously in attacks.

"Also there is a little bit harmless source code of polymorphic x86/x64 modular EPO file infector m0yv detected in the wild as Win64/Expiro virus, but it is not expiro actually, but AV engines detect it like this, so no single thing in common with gazavat," the ransomware developer said in the forum post.

"M0yv source is a bonus, because there was no any major source code of resident software for years now, so here we go," the developer later explained.

This source code come in the form of a Microsoft Visual Studio project and includes some already compiled DLLs.



```
// основная работа инфектора в активном состоянии
// по завершению работы спит N времени и освобождает ownership мьютекса
// позволяя инфекторам в других процессах перейти в активное состояние
// одновременно может быть только 1 поток с активным инфектором
// период ожидания нужен, чтобы были периоды неактивности между активными фазами в разных процессах
VOID InfectorActiveJob(capsid_metadata *capsid, BOOL bInfectLocal, BOOL bInfectNetwork)
{
    // mutex на handle владельцем которого мы будем являться после ожидания
    HANDLE hInfectorMutex = NULL;
    for (;;)
    {
        if (sync::CreateMutexAndWait(sync::sync_type_t::SYNC_INFECTOR, &hInfectorMutex))
            break;

        Sleep(10 * 1000); // если у нас не удалось войти в режим ожидания по какой-либо причине, то будем повторять
        каждые 10 секунд пока не получится
    }

    capsidProcessingForm processingData;
    ITraverse *traverser = nullptr;

    RtlSecureZeroMemory(&processingData, sizeof(processingData));
    processingData.capsid = capsid;

#ifdef _PATH_INFECTOR_NOSEARCH
    search_api::search_parameter param;
    RtlSecureZeroMemory(&param, sizeof(param));
    param.bExitThread = FALSE;
    param.bUseBlacklist = TRUE;
    param.dwParameterSize = sizeof(capsidProcessingForm);
    param.lpParameter = (LPBYTE)&processingData; // передавать каждому препроцессингу
    param.onFound = preprocessing::ProcessFile;
    param.pwEntrySearch = L"C:\\inf_test\\bins";
```

Source code snippet for the M0yv malware

Source: BleepingComputer

The todo.txt file indicates the source code for this malware was last updated on January 19th, 2022.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

Practice your development skills with lifetime access to DevDojo

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Decryption Key
- Developer
- Egregor
- Maze
- Ransomware
- Sekhmet

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

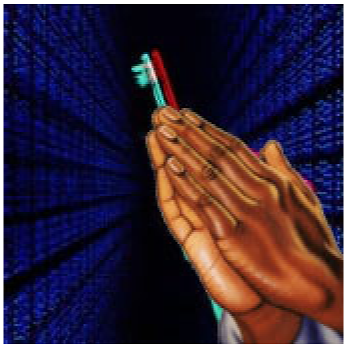
Comments

-
  mynameisgod - 3 months ago
  -
  -

  Awww bless his heart. What a kind and caring criminal he is.

-
  TsVk! - 3 months ago
  -
  -

  A smart criminal knows when it's time to cash in and walk away. Releasing the keys wasn't necessary, I'm glad that many will be able to get their files back now.

- 

  DG1991 - 3 months ago

  I hope the guys from STOP/DJVU Ransomware gang will do the same thing in the future, *praying.

-

  vnabc - 3 months ago

  Hopefully, Phobos group would do the same soon!

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: