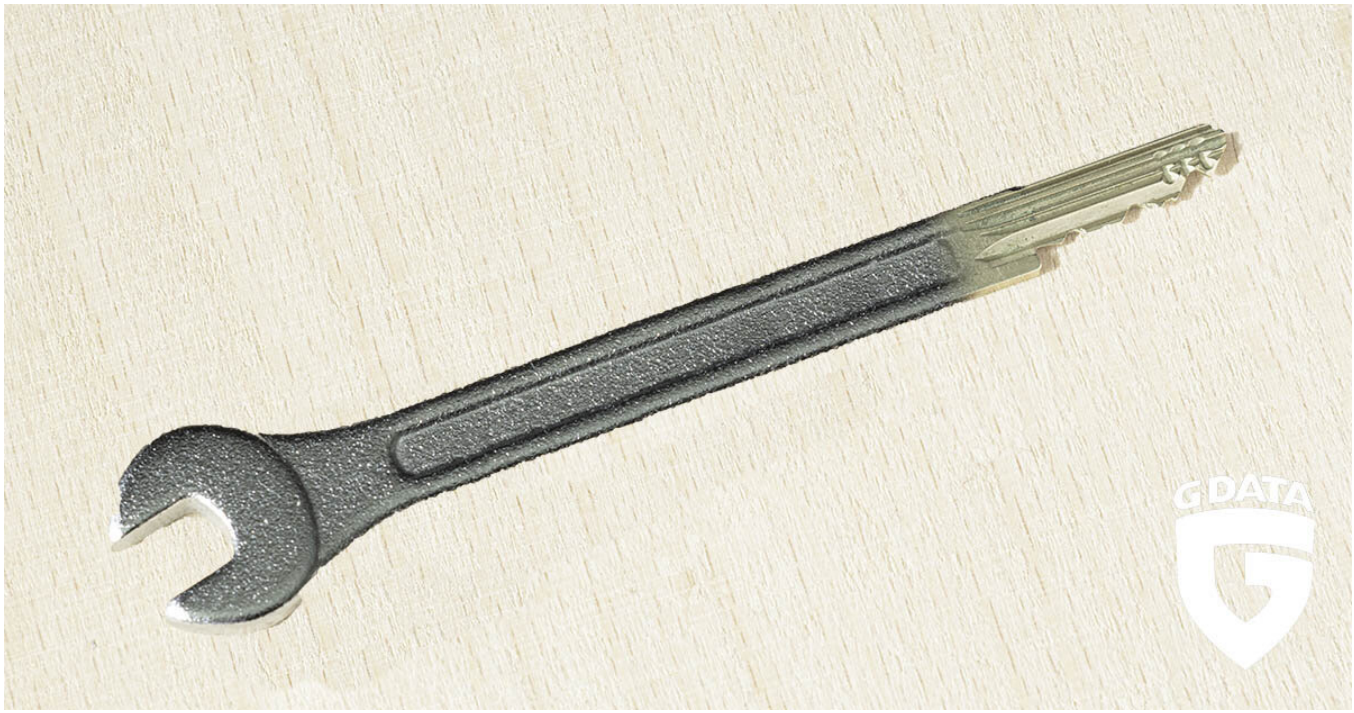
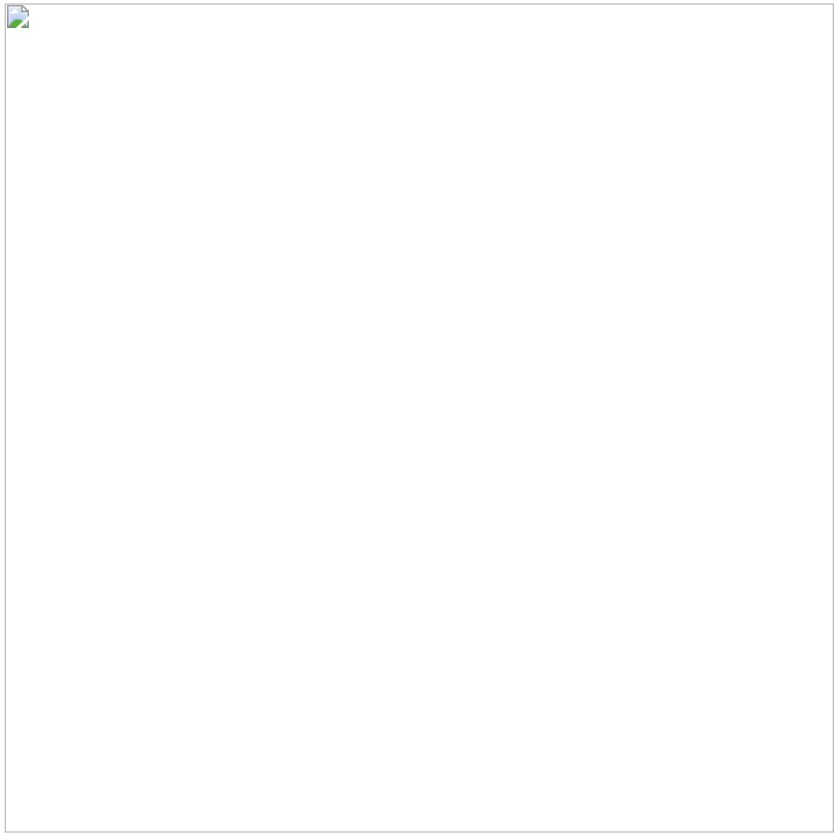
DLL Fixer leads to Cyrat Ransomware

gdatasoftware.com/blog/cyrat-ransomware



A new ransomware uses an unusual symmetric encryption method named "Fernet". It is Python based and appends .CYRAT to encrypted files.

Discovery & Initial Analysis



While hunting for new malware we often use Yara rules to find suspicious samples. One of my generic ransomware hunt rules found this new ransomware sample. At the time it had only 2 detections on Virustotal. The first submission date is 25. August 2020.

DiE and PortexAnalyzer note that there is a zlib archive in the overlay of the file. Further inspection shows references to the python37.dll and the archive's name PYZ-00.pyz which is typical for PyInstaller executables.

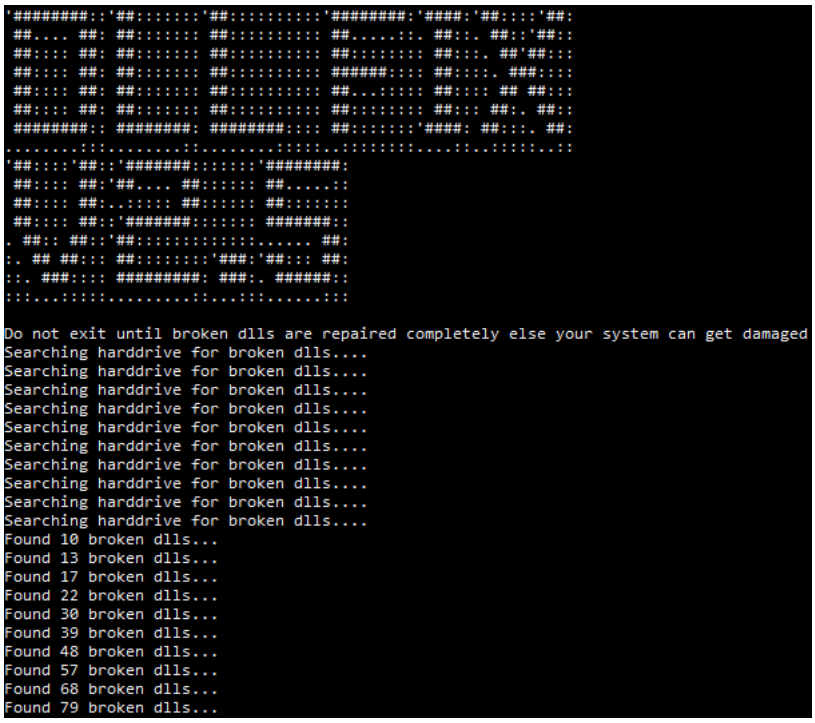
It means Cyrat ransomware was compiled with Python 3.7 and converted to a Windows PE file using PyInstaller.

Unpacking and decompiling this file requires PyInstxtractor, Python 3.7 and, e.g., uncompyle6. The Python version needs to be the same as the malware executable while extracting the .pyc files. Otherwise PyInstxtractor has issues properly constructing the files.

Disguise as DLL fixer

When I first tried to run the malware it crashed because of a missing fonts for pyfiglet. To see it in action, I had to install pyfiglet and replicate the code that displays the ransomware's output.

The malware disguises as DLL fixer 2.5 (see image below). Upon execution it will display a randomly created number of corrupted DLLs it pretends to have found on the system. After the system has been encrypted, a success message for fixing the DLLs is shown.



Encryption

Cyrat ransomware uses Fernet to encrypt files. This is a symmetric encryption method meant for small data files that fit into RAM. While Fernet is not unusual itself, it is not common for ransomware and in this case even problematic. This ransomware encrypts whole files regardless how big they are, whereas Fernet is unsuitable for big files.

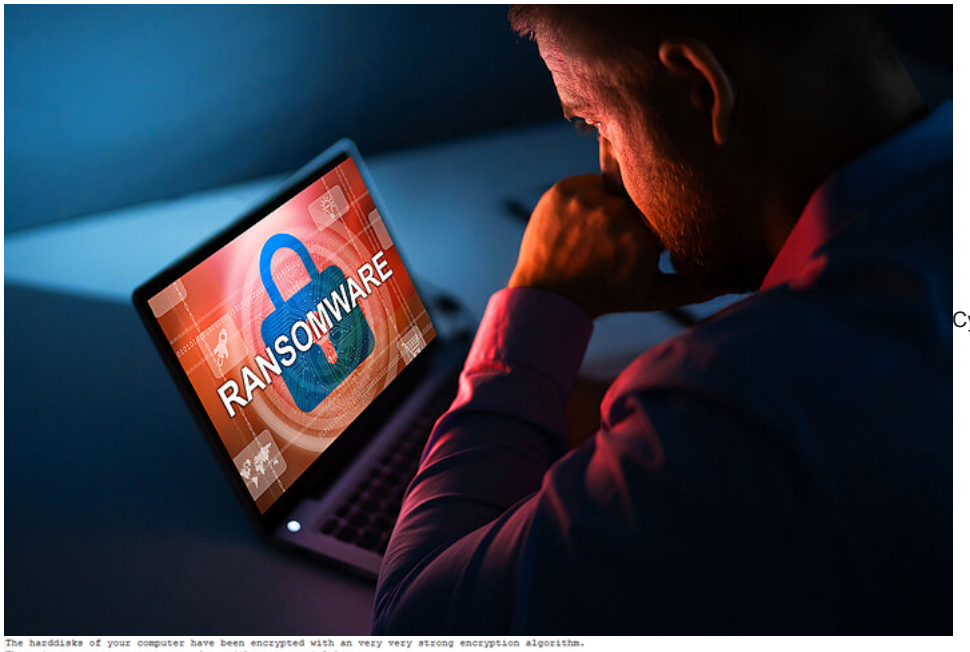
A public RSA key is used to encrypt the Fernet key. This public key is downloaded from Mediafire instead of shipping it with the ransomware. This adds another dependency. The encrypted Fernet key is saved in **Desktop\EMAIL_US.txt**. A user with an infected system is required to send this file to the criminals.

Cyrat appends **.CYRAT** to encrypted files. It has a list of folders that it checks for target files. Those folders are 'Desktop', 'Downloads', 'Pictures', 'Music', 'Videos', and 'Documents'.

It targets files with the following extensions: 'doc', 'docx', 'xls', 'xlsx', 'ppt', 'pptx', 'boop', 'pst', 'ost', 'msg', 'eml', 'vsd', 'vsdx', 'txt', 'csv', 'rtf', '123', 'wks', 'wk1', 'pdf', 'dwg', 'onetoc2', 'snt', 'jpeg', 'jpg', 'docb', 'docm', 'dot', 'dotm', 'dotx', 'xlsm', 'xlsb', 'xlw', 'xlt', 'xlm', 'xlc', 'xltx', 'xltm', 'pptm', 'pot', 'pps', 'ppsm', 'ppsx', 'ppam', 'potx', 'potm', 'edb', 'hwp', '602', 'sxi', 'sti', 'sldx', 'sldm', 'sldm', 'vdi', 'vmdk', 'vmx', 'gpg', 'aes', 'PAQ', 'bz2', 'tbk', 'bak', 'tar', 'tgz', 'gz', '7z', 'rar', 'zip', 'backup', 'iso', 'vcd', 'bmp', 'png', 'gif', 'raw', 'tif', 'tiff', 'nef', 'psd', 'ai', 'svg', 'djvu', 'm4u', 'm3u', 'mid', 'wma', 'flv', '3g2', 'asf', 'mpeg', 'vob', 'mpg', 'swf', 'wav', 'mp3', 'sh', 'class', 'jar', 'java', 'rb', 'asp', 'php', 'jsp', 'brd', 'dch', 'dip', 'pl', 'vb', 'vbs', 'ps1', 'bat', 'cmd', 'asm', 'h', 'pas', 'c', 'cs', 'suo', 'sln', 'ldf', 'mdf', 'ibd', 'myi', 'myd', 'frm', 'odb', 'dbf', 'db', 'mdb', 'accdb', 'sql', 'sqlitedb', 'sqlite3', 'lay6', 'lay', 'mml', 'sxm', 'otg', 'odg', 'uop', 'std', 'sxd', 'otp', 'odp', 'wb2', 'slk', 'dif', 'stc', 'sxc', 'ots', 'ods', '3dm', 'max', '3ds', 'uot', 'stw', 'sxw', 'ott', 'odt', 'p12', 'csr', 'key', 'pfx', 'der', 'deb', 'mpeg', 'WEBM', 'MPG', 'MP2', 'MPEG', 'MPE', 'MPV', 'OGG', '3gp', 'mp3', 'json', 'css', 'html', 'py', 'exe', 'MP2', 'MPEG', 'MPE', 'MPV', 'OGG', '3gp', 'mp3'

The ransomware lists a few more extensions with a dot in them which is a bug: '.ARC', '.cpp', '.cgm', '.js', '.fla', '.asc', '.crt', '.sch'. These extensions will never be found by Cyrat because the file path is stripped from dots before it is compared with the target extension.

A ransom note named **RANSOME_NOTE.txt** is placed in every target folder. Furthermore a ransomware stock photo is downloaded from **images.idgesg.net** to **Documents\background_img.png** and set as wallpaper. The wallpaper does not contain any ransom message. In this state the stock photo's only purpose is to draw attention to the user.



Cyrat sets this stock photo as wallpaper

```
The harddisks of your computer have been encrypted with an very very strong encryption algorithm.
There is no way to restore your data without a special key.
Only we can decrypt your files!
To purchase your key and restore your data, please follow these three easy steps:

1. Email the file called EMAIL_US.txt at Desktop\EMAIL_US.txt to officialintuitsoftware@gmail.com

2. You will recieve your personal BTC address for payment.
Once a payment of $1000 in btc has been completed, send another email to officialintuitsoftware@gmail.com Titled "PAID".
We will check to see if payment has been paid.
Note: If you make your payment within 2 days, the fees would be slashed by half, that is $500 in btc

3. You will receive a text file with your KEY that will unlock all your files. You have 2 days from today being Aug-27-2020
IMPORTANT: To decrypt your files, place text file on desktop and wait. Shortly after it will begin to decrypt all files.

WARNING:
Do NOT attempt to decrypt your files with any software as it is obselete and will not work, and may cost you more to unlock your files.
Do NOT change file names, mess with the files, or run decryption software as it will cost you more to unlock your files and Your files might be lost forever.
Do NOT send "PAID" without paying, price will double for disobedience.
Do NOT think that we won't leave your files encrypted forever because we will"
Don't know what btc is? Visit https://bitcoin.org
```

Cyrat's ransom note (click to enlarge)

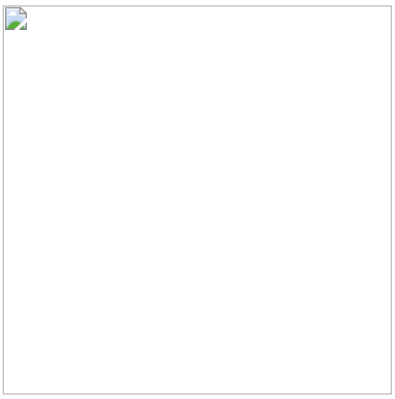
Registry Changes and Persistence

The ransomware deletes shadow volume copies and disables CMD, taskmanager, regstry tools via policy settings in the registry. It also removes the RUN command from the start menu and task manager. It uses bcedit to set **recoveryenabled** to **No** and **bootstatuspolicy** to **ignoreallfailures**

For persistence Cyrat copies itself to the autostart folder **\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**

A reboot of the system, and thus re-run of the rasomware, will most likely encrypt the ransom notes. I did not find any safeguard in the code to prevent this from happening.

Target Platforms



The target platform is undoubtedly Windows because the PyInstaller executable only works there. The trojanized DLL fixer will only lure Windows users. Registry commands and persistence mechanisms are also Windows based.

Oddly, there are also checks for Linux and Darwin (core of many Apple operating systems) in the main body without any changes in the following code which is still Windows targeted.

Contacting the Threat Actor(s)

After I posted the Cyrat sample on Twitter, another Twitter user, who wants to be referred to as **alex27**, contacted the ransomware crook(s). He asked them for decryption and shared their email exchange with me. This shows that the threat actor(s) are expecting help requests from affected users, and thus, actively distributing the malware.

> We got your message, calm down your files are safe you will only get them back if you obey and follow the instruction. You know about bitcoin now? Did The page we put there to help you get bitcoin help? If no you can use google and find how to get bitcoin in your country and get $1,000 worth of bitcoin sent to this bitcoin address: <redacted> Your two days count start now, we have full access to your computer and we know you are reading this now. $500 will be added each day once the two days elapse and you didn't make payment for the decryptor. Don't think we won't delete those files if we don't hear from you because we will.

I redacted the bitcoin address because it is likely individually created for every case. It has currently no transactions. **alex27** pointed out that their responses as well as the ransom note contain many grammar mistakes, making it unlikely that the author is a native English speaker.

Conclusion

As it is often the case with brand new malware discoveries, this sample is buggy and not yet ready to infect any system because it crashes in it's current state. However, the threat actor's reply shows they are active and might have already published versions that work. It's usually just a matter of time until those flaws are fixed. The problematic choice of the Fernet encryption method may take its toll on systems while they try to encrypt gigabyte sized files in RAM all at once.

Some parts of the code show an intention of also infecting Darwin and Linux systems, which may be added later on.

Unfortunately, there is currently no known way to decrypt files without the key.

Indicators of Compromise

Description	Filename	Hash/URL
Ransomware executable	NA	4b76ad80e9ce4c503bde0e476a88447426fc38315d440d22926627295e1b0ec6
Ransomnote	RANSOME_NOTE.txt	generated per execution
RSA public key	\Documents\pub_key.pem	hxxp://download1582.mediafire.com/c91ywpc4l7ag/xj26578psz6n9xo/public_key.pem
Raw/plain Fernet key file	\Documents\key.txt	generated per execution
Encrypted Fernet key file	EMAIL_US.txt	generated per execution
Wallpaper	\Documents\background_img.png	hxxps://images.idgesg.net/images/article/2020/05/ransomware_attack_worried_businessman_1199291222_cso_2400x1600-100840844-large.jpg