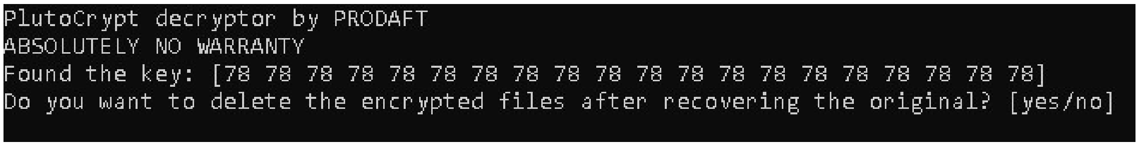
PRODAFT

Decrypted: PlutoCrypt Ransomware

How does it work?

PlutoCrypt encrypts files with a randomly generated key which has a 20-byte key size. The encryption is byte addition with this key. The decryptor performs a known plaintext attack, and the plaintext is !This program cannot be run in DOS text sequence that starts at position 77 of the Windows executables. Since it is longer than 20 bytes, it is more than enough for recovering the key.

Note: Due to a wrong implementation of PlutoCrypt's encryption function, the effective key size is 1 byte rather than 20 bytes. Hence, when the decryptor is running, the found key will have the same byte size. An example screenshot is given below. However, in case of any future development of the malware, we have implemented the decryptor with the assumption that the key size is still going to be 20 bytes.



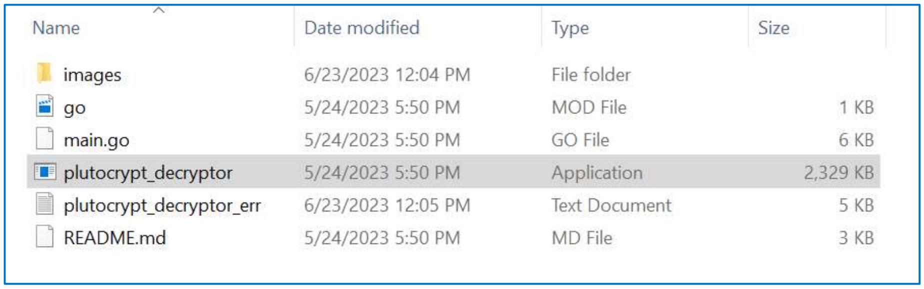
```
PlutoCrypt decryptor by PRODAFT
ABSOLUTELY NO WARRANTY
Found the key: [78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78 78]
Do you want to delete the encrypted files after recovering the original? [yes/no]
```

How to run the decryptor?

1. Download the decryptor executable from the following Link: https://github.com/prodaft/malware-ioc/raw/master/PlutoCrypt/plutocrypt_decryptor.exe

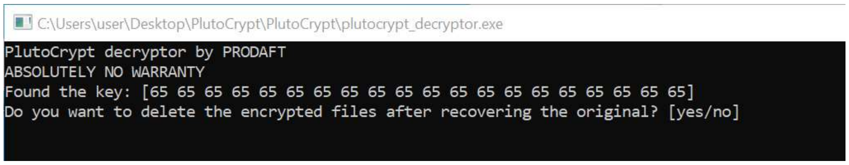
2. Move the executable to your infected machine.

3. Run the executable by double clicking,



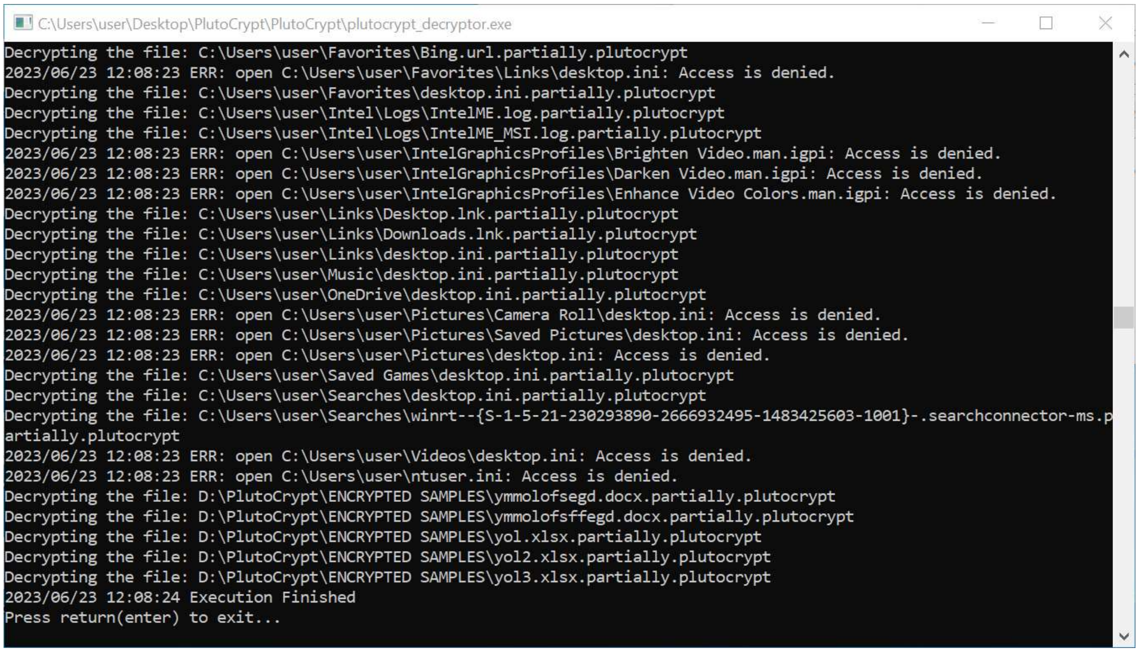
Name	Date modified	Type	Size
images	6/23/2023 12:04 PM	File folder	
go	5/24/2023 5:50 PM	MOD File	1 KB
main.go	5/24/2023 5:50 PM	GO File	6 KB
plutocrypt_decryptor	5/24/2023 5:50 PM	Application	2,329 KB
plutocrypt_decryptor_err	6/23/2023 12:05 PM	Text Document	5 KB
README.md	5/24/2023 5:50 PM	MD File	3 KB

4. The executable will ask you to keep the encrypted files or delete them. Answer that question with a yes or no depending on your preference.


C:\Users\user\Desktop\PlutoCrypt\PlutoCrypt\plutocrypt_decryptor.exe

```
PlutoCrypt decryptor by PRODAFT
ABSOLUTELY NO WARRANTY
Found the key: [65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65]
Do you want to delete the encrypted files after recovering the original? [yes/no]
```

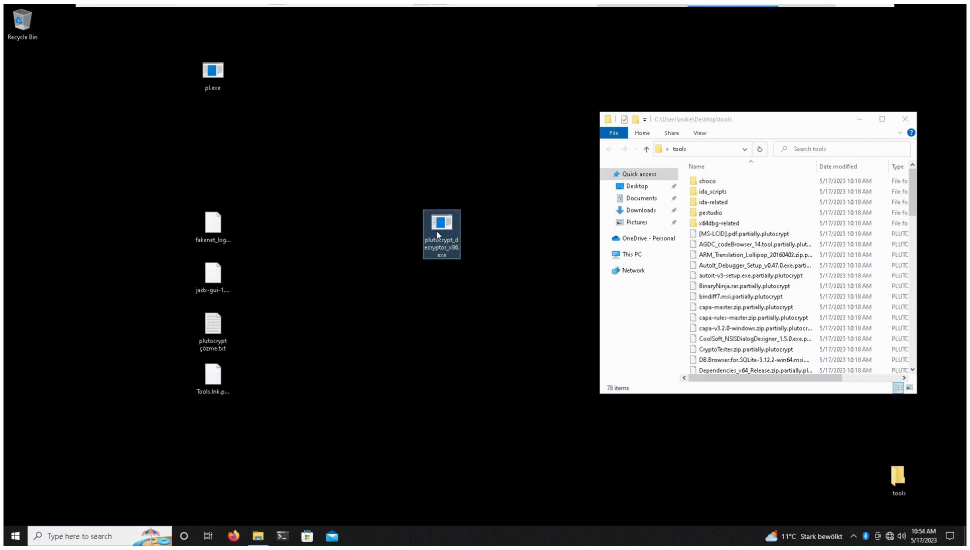
5. When the execution is finished, press enter to exit.


C:\Users\user\Desktop\PlutoCrypt\PlutoCrypt\plutocrypt_decryptor.exe

```
Decrypting the file: C:\Users\user\Favorites\Bing.url.partially.plutocrypt
2023/06/23 12:08:23 ERR: open C:\Users\user\Favorites\Links\desktop.ini: Access is denied.
Decrypting the file: C:\Users\user\Favorites\desktop.ini.partially.plutocrypt
Decrypting the file: C:\Users\user\Intel\Logs\IntelME.log.partially.plutocrypt
Decrypting the file: C:\Users\user\Intel\Logs\IntelME_MSI.log.partially.plutocrypt
2023/06/23 12:08:23 ERR: open C:\Users\user\IntelGraphicsProfiles\Brighten Video.man.igpi: Access is denied.
2023/06/23 12:08:23 ERR: open C:\Users\user\IntelGraphicsProfiles\Darken Video.man.igpi: Access is denied.
2023/06/23 12:08:23 ERR: open C:\Users\user\IntelGraphicsProfiles\Enhance Video Colors.man.igpi: Access is denied.
Decrypting the file: C:\Users\user\Links\Desktop.lnk.partially.plutocrypt
Decrypting the file: C:\Users\user\Links\Downloads.lnk.partially.plutocrypt
Decrypting the file: C:\Users\user\Links\desktop.ini.partially.plutocrypt
Decrypting the file: C:\Users\user\Music\desktop.ini.partially.plutocrypt
Decrypting the file: C:\Users\user\OneDrive\desktop.ini.partially.plutocrypt
2023/06/23 12:08:23 ERR: open C:\Users\user\Pictures\Camera Roll\desktop.ini: Access is denied.
2023/06/23 12:08:23 ERR: open C:\Users\user\Pictures\Saved Pictures\desktop.ini: Access is denied.
2023/06/23 12:08:23 ERR: open C:\Users\user\Pictures\desktop.ini: Access is denied.
Decrypting the file: C:\Users\user\Saved Games\desktop.ini.partially.plutocrypt
Decrypting the file: C:\Users\user\Searches\desktop.ini.partially.plutocrypt
Decrypting the file: C:\Users\user\Searches\winrt--{S-1-5-21-230293890-2666932495-1483425603-1001}-.searchconnector-ms.p
artially.plutocrypt
2023/06/23 12:08:23 ERR: open C:\Users\user\Videos\desktop.ini: Access is denied.
2023/06/23 12:08:23 ERR: open C:\Users\user\ntuser.ini: Access is denied.
Decrypting the file: D:\PlutoCrypt\ENCRYPTED SAMPLES\ymmolofsegd.docx.partially.plutocrypt
Decrypting the file: D:\PlutoCrypt\ENCRYPTED SAMPLES\ymmolofsffegd.docx.partially.plutocrypt
Decrypting the file: D:\PlutoCrypt\ENCRYPTED SAMPLES\yol.xlsx.partially.plutocrypt
Decrypting the file: D:\PlutoCrypt\ENCRYPTED SAMPLES\yol2.xlsx.partially.plutocrypt
Decrypting the file: D:\PlutoCrypt\ENCRYPTED SAMPLES\yol3.xlsx.partially.plutocrypt
2023/06/23 12:08:24 Execution Finished
Press return(enter) to exit...
```

6. Some files may not be recovered due to certain permissions. In that case, these errors will be logged into the plutocrypt_decryptor_err.log file located in the same position as the executable. It is recommended to read that log file after the execution.

7. A sample execution is given below



Name	Date modified	Type
choco	5/17/2023 10:18 AM	File fo
ida_scripts	5/17/2023 10:18 AM	File fo
ida-related	5/17/2023 10:18 AM	File fo
pestudio	5/17/2023 10:18 AM	File fo
x64dbg-related	5/17/2023 10:18 AM	File fo
[MS-LCID].pdf.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
AGDC_codeBrowser_14.tool.partially.plut...	5/17/2023 10:18 AM	PLUTC
ARM_Translation_Lollipop_20160402.zip.p...	5/17/2023 10:18 AM	PLUTC
AutoIt_Debugger_Setup_v0.47.0.exe.parti...	5/17/2023 10:18 AM	PLUTC
autoit-v3-setup.exe.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
BinaryNinja.rar.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
bindiff7.msi.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
capa-master.zip.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
capa-rules-master.zip.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
capa-v3.2.0-windows.zip.partially.plutocr...	5/17/2023 10:18 AM	PLUTC
CoolSoft_NSISDialogDesigner_1.5.0.exe.p...	5/17/2023 10:18 AM	PLUTC
CryptoTester.zip.partially.plutocrypt	5/17/2023 10:18 AM	PLUTC
DB.Browser.for.SQLite-3.12.2-win64.msi....	5/17/2023 10:18 AM	PLUTC
Dependencies_x64_Release.zip.partially.pl...	5/17/2023 10:18 AM	PLUTC