Exposing the Iranian EvilNominatus Ransomware

Introduction

As part of our monitoring of malicious files in current use, we detected a malicious BAT file that was uploaded to VirusTotal from Iran. This file executes a ransomware that we associated with the EvilNominatus ransomware, initially exposed at the end of 2021. It seems that the ransomware's developer is a young Iranian, who bragged about its development on Twitter.

At this point, we have no details regarding any victims of this ransomware. We publish this research due to the malware’s unique method of operation, and the low number of AV engines capable of detecting it.

The original BAT file the research is based on was only detected by two AV engines on VirusTotal. Another BAT file that was discovered later, which shares characteristics with the first one, wasn't detected by any AV engines. Other files that were either generated by the BAT files or communicated with them to carry out attacks were detected by multiple AV engines. Therefore, we assess that the tool's general level of risk is low at this point.

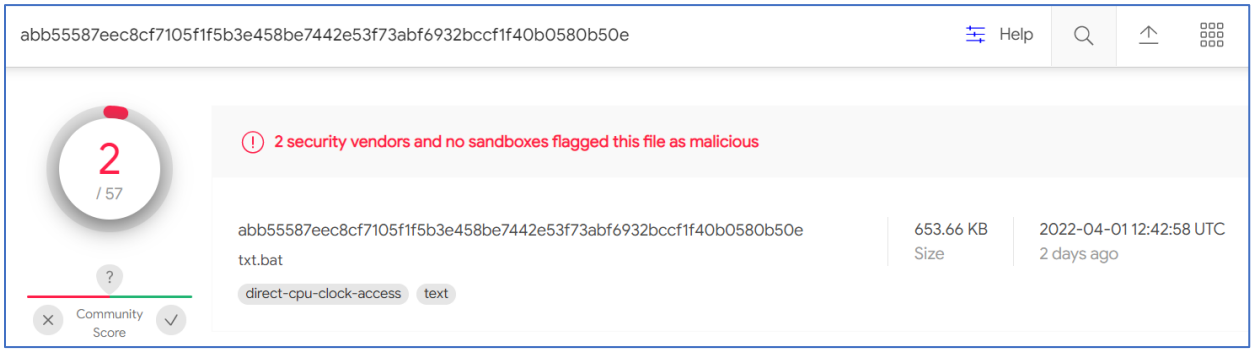
Following is the BAT file, 650KB in size, in its encoded form:

The encoded BAT file can download additional malicious files, deleting shadow copies, encrypting files, cancelling the registry edit tool, as well as multiple other capabilities that will be discussed in this report. The report will also provide details concerning the ransomware's developer, their email address, and their username on Discord and Twitter.

Investigating the File

The file was uploaded from Iran on 01.04.2022:

File Name: txt.bat
File Type: bat
MD5: d3f480c79a3964fa26033d19d9fbd661
SHA-1: 0afc1b886e12e22e01ded0ae87e2caa5d5a99363
SHA-256: abb55587eec8cf7105f1f5b3e458be7442e53f73abf6932bccf1f40b0580b50e



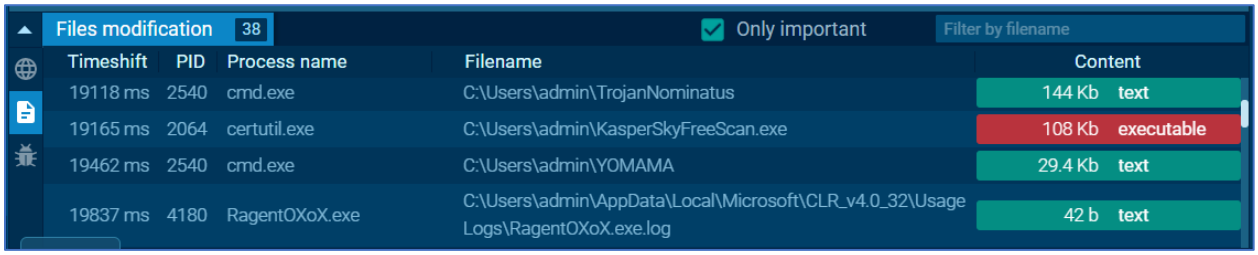
A **static investigation** of the file refers to the following URL:

hxxps[:]//i-love-evilnominatuscrypt[.]000webhostapp[.]com/GoogleAlert[.]vbs

The URL has no AV detections – 0/93. The "GoogleAlert.vbs" file located on the URL is flagged by 19 out of 53 AV engines.

Dynamic Investigation

During the dynamic investigation of the BAT file, a number of files were generated, each responsible for several actions:



A screenshot with a partial list of the generated files

1. An executable named "AntivirusScan.exe" was generated. The file's hash on VirusTotal is detected as malicious by 49 out of 68 AV engines, and it is named "EvilNominatusCrypto.exe". The file modifies Windows' LOGIN/LOGOFF path on the registry. This modification prevents users from accessing the Taskbar.
2. A TXT file named "XoX" was generated. The file is encoded and decrypted by Windows' Certutil. It is possible that the "XoX" file is designed to execute the "AntivirusScan.exe" file.

3. Actions carried out by the BAT file:
   - It generates a file named "RagentOXoX.exe" that downloads a file named "crash.bat" to establish persistence: C:\Users\admin\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\Crash.bat
   - It reads the computer's name.
   - It examines the supported languages on the system (the file does not seem to change its behavior according to this check).
4. A malicious file named "Nod32Installer.exe" is downloaded. This file impersonates ESET's security product for computers. This file's hash is detected by 15/68 AV engines on VirusTotal.
5. A malicious file named "KasperskyFreeScan.exe" is generated via the certutil.exe process. The malicious file impersonates the name of Kaspersky's security product as well.
6. All TXT files are Base64-encoded. Before their execution, the malicious files use the certutil service to decode via the decrypt command. Base64 encoding is used by malware to prevent AV engines from detecting malicious strings.

Additional Activity by Downloaded or Generated Files

The ransomware deletes the computer's Shadow Copy to prevent recovery:

Command Line:

```
"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet && wm
ic shadowcopy delete
```

"AntivirusScan.exe" disables the option to use Registry Editing Tools:

Command Line:

```
"C:\Windows\System32\cmd.exe" /C reg add HKCU\Software\Microsoft\Windows\C
urrentVersion\Policies\System /v DisableRegistryTools /t REG_DWORD /d 1 /f
```

"AntivirusScan.exe" also disables access to the network and Firewall:

Command Line:

```
"C:\Windows\System32\cmd.exe" /C net stop Windows Firewall
```

Command Line:

```
"C:\Windows\System32\cmd.exe" /C net stop Network Connections
```

In case the files encounter a problem while running, a Word file is opened to display the following text to the user:
"*Make sure your antivirus is off and macro is not disabled. If it is not disabled, click ENABLE CONTENT button or this text will not work!!!!"*

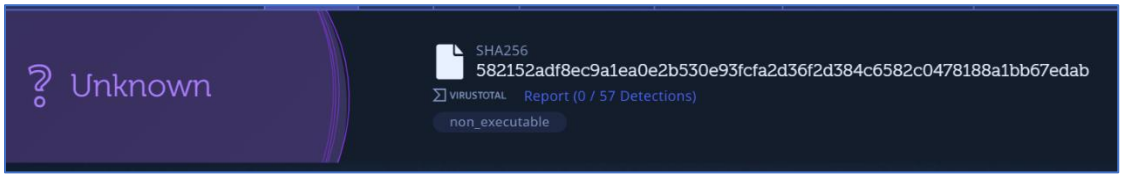
When the machine is fully encrypted, files receive the ".ink-locked" extension, and the ransom note is displayed:

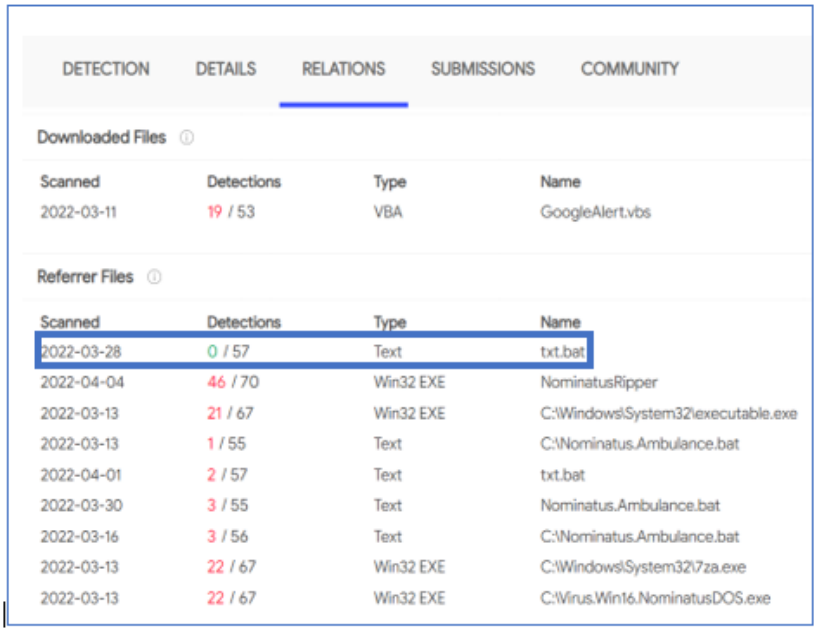
If the wrong value is entered to the "code" field three times, the prompt disappears, leaving files encrypted indefinitely.
The message refers to the attacker's email address: Bkhtyarywzbh@gmail[.]com, but investigating this address provided no further findings.

Exposing and Investigating an Additional BAT File

When investigating the URL hxxps://i-love-evilnominatuscrypt[.]000webhostapp[.]com/GoogleAlert[.]vbs, we detected a few additional files that communicate with it. An additional BAT file with 0 detections on VirusTotal and Intezer was detected among these files. Dynamically executing the file indicates that it is the same ransomware file, with the same capabilities as described above.
The file's details:

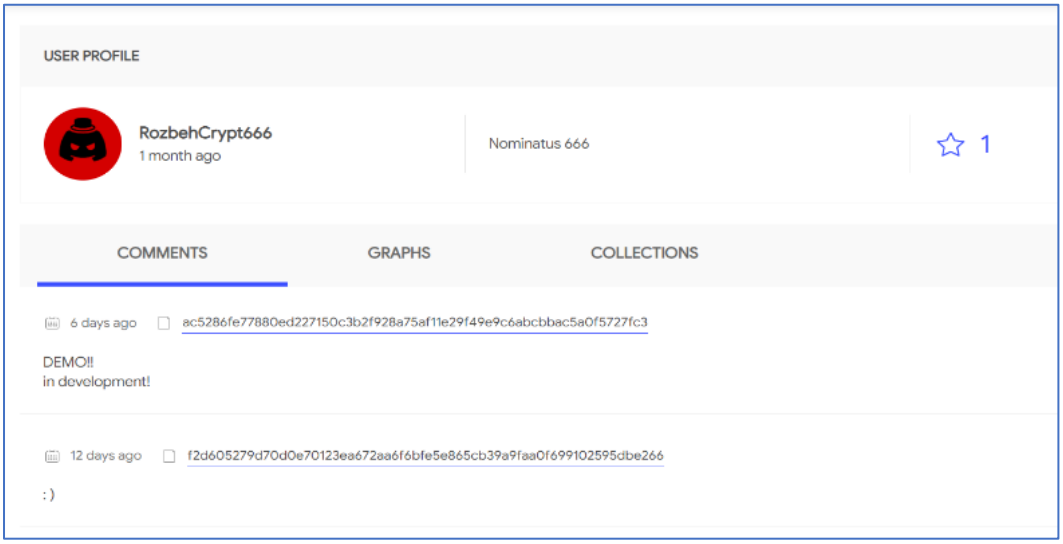
File Name: txt.bat
File Type: bat
MD5: 765d27aede93251a79d7685c7403a70b
SHA-1: 3c8d4a0d6590bc0e632cde0c93d9da09194e118a
SHA-256: 582152adf8ec9a1ea0e2b530e93fcfa2d36f2d384c6582c0478188a1bb67edab

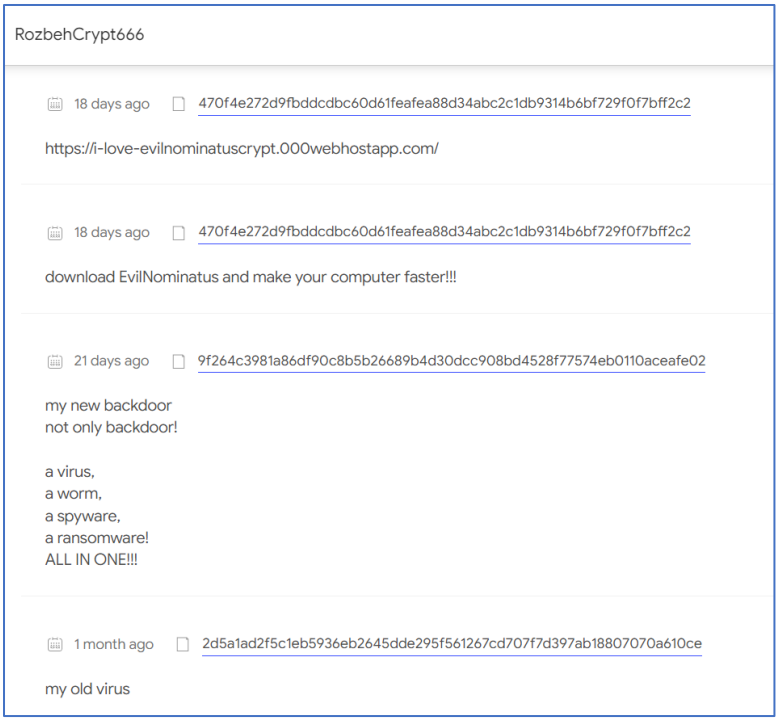




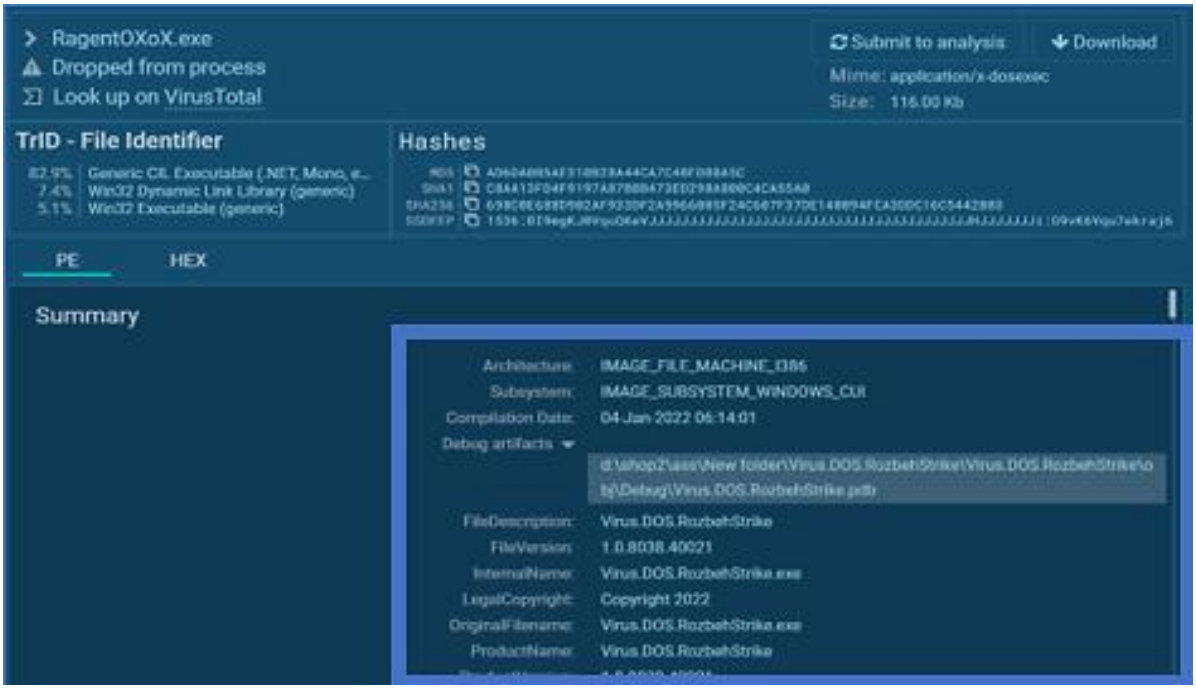
Attribution to the Ransomware's Developer

One of the files that communicate with the BAT file is Nod32Installed.exe. When searching for this file on VirusTotal, we discovered a user named "RozbehCrypt666", claiming credit for the ransomware.
The user's profile on VirusTotal is the following:





A file named "RagentOXoX.exe" was generated during the BAT file's execution. While examining "RagentOXoX.exe" we found out that the file's name was "Virus.DOS.**RozbehStrike**". This name resembles the username that claimed credit for the ransomware on VirusTotal – "**Rozbeh**Crypt666".



Checking the name "Rozbeh" on Google showed that this is a traditional Persian name, meaning "a good day":

Roozbeh or Rouzbeh (Persian: روزبه) is an **old Persian male given name** . The name consists of the words "rooz" (day) and "beh" (better) and it means "fortunate". Persons named Roozbeh include: Rhahzadh "Roch Vehan" (Rōzbehān), son of a certain Rōzbeh. Rouzbeh (died 653/656), given name of Salman the Persian.

Meaning: fortunate, good day

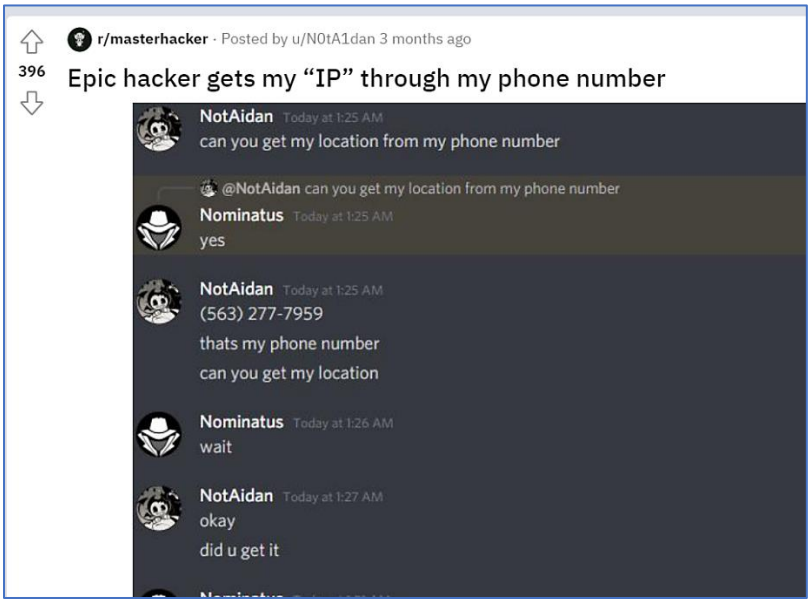
https://en.wikipedia.org › wiki › Roozbeh

Roozbeh - Wikipedia

After running the malicious BAT files, a file named "YOMAMA" was downloaded, containing the following information:

```
....".p.i.c.t.u.r.e.B.o.x.1...I.m.a.g.e.....Oops your Computer Locked by
NominatusLocker! you have 1 hour left to Get the Special key from creator of
this Virus Bkhtyaryrwzbh@gmail.com! or we will Destroy your Computer or you can
Contact him on discord Nominatus#1297 live or death? MAKE YOUR CHOICE
NOW!!@.....ÿÿÿÿ.............QSystem.Drawing, Version=4.0.0.0, Culture=neutral,
```

The attacker refers to a Discord user named "Nominatus#1297". An OSINT investigation of the Discord account revealed the following Reddit thread:



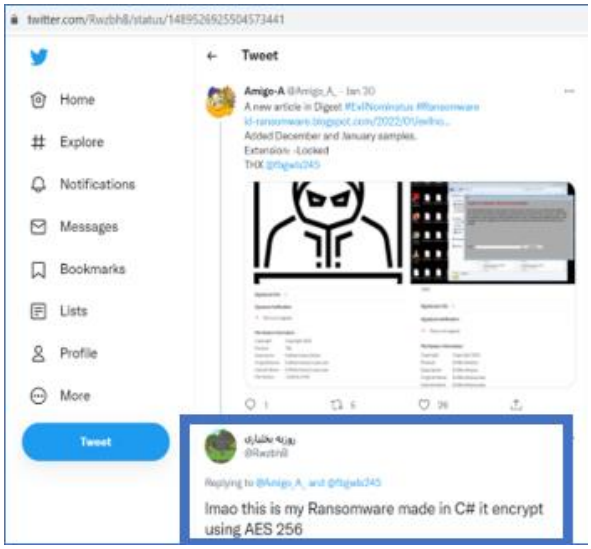
However, since the full ID does not appear next to the username, it is hard to say with high certainty whether this is the same user.

When examining the malicious "Nod32.Installer" file, we detected a string named "Minecraft 2d":

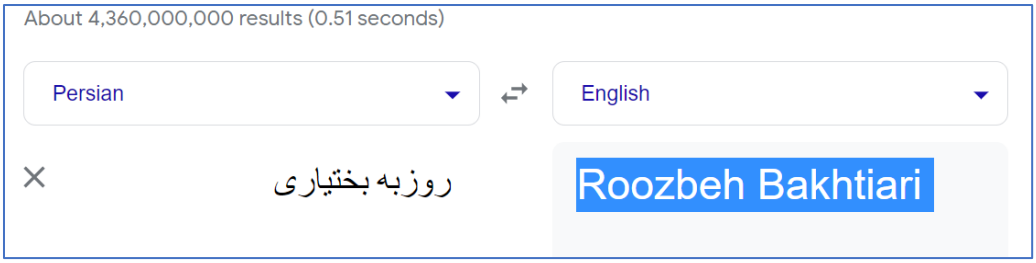
```
FileVersion
2.1.0.0
ProductVersion
LegalCopyright
Comments
Minecraft 2d
VarFileInfo
Translation
```

Investigating the Ransomware's Name - EvilNominatus

While investigating the ransomware's name, we discovered that its name was apparently taken from an episode of the series Nominatus Rising – Sonic Boom, season 2, episode 23.
Notably, all detected file names ("YOMAMA" and "Nominatus", from the Sonic Boom series) as well as the string found under the name "Minecraft 2d", indicate an association with young gamers.
A user with a Persian name identical to the one on VirusTotal was detected on Twitter, taking responsibility for the ransomware:



The user's Twitter profile image was taken from the computer game Minecraft.



The Twitter username transliterated from Persian via Google Translate

Indicators of Compromise (IoCs):

URL:
hxxps[:]//i-love-evilnominatuscrypt[.]000webhostapp[.]com/GoogleAlert[.]vbs

SHA256:
E09B43312A6B1622428A3D8BAB0270673701D7D7A73C667DC3EE8940DA0B96A1
69811A6C9376B219B335A055CFA970D38CD768ABECA7138A2C1905560D468FEF
EFC85A4100DAE0D3FA69CFF22149A3F735EE34BB43C79524F379C44AC5814751
1D2A96013E4CC499CFFAB9000B9595E532A9FEEE425D3B4F536A5DC0695F381B
98A9C760BB94D4D081271A3087ACE8BED47FC4C8A38CDFE3F42B92BCDBEE68E7
698C0E688D902AF933DF2A9966005F24C607F37DE140094FCA3DDC16C5442B03
9062660482465279DE6EB783B5CFFF8BB1F1BD804E0D8BF0876897B07407308B
B93247A0EFBBB9852D056E8CB655FC76D802928BF23586077EF0D73BA710E514
E21FE7117B2BCA120DEC9F0BD970A6355B143A3B62207B480F93D1E35B70C0E5
1EE21714BDE9BF89CC6C55D7DAC5686AD0E85F231C2BA7F91D575CB6A1F8092E
4E99E6B477DAA5717A97F12A01EE8F2FA5AA8DCE870982C7C45382C0E73AA1D1
582152adf8ec9a1ea0e2b530e93fcfa2d36f2d384c6582c0478188a1bb67edab

SHA1:
CC4EA1BAB6496272566EBDC6823A7EB27A52A727
0170C2DEAE4486A43894C202EA92D43556218E1C
B2BE8A2F8039404070636759E9E3D618B3A15F56
AC1DA853F09D338053C2F4901F157CBCB6729BED
4D536DC808FCED63ADBC36ADAF772554B64E49DF
C8AA13FD4F9197A87BBB473ED298A800C4CA55A0
7F30A37552FE7D82BBB149F0877BA2D2B7E4ACB8
66501D433C3E0FCAB32DA325EBC6E20192A2294B
08CA0BD79D92A8F89D8714B29B695C8CC53F90FC
6895E15111ECB3976D95622588E2D775A0F48870
287E080B63FEF822370BCE236031620B8E421D14
3c8d4a0d6590bc0e632cde0c93d9da09194e118a

MD5:
EC0648563F5EAD6ABA26D59B741F8A73

7CDF50EE4F3D0FEBC70DD36298ED07DA
FC70E3C1D3082CBCF48AC94700A84AC9
98831A06B42B18076EFA52A9D03CF5A8
7E055FBB0834B0484196A792576B47C0
AD6DA0B5AE310B28A44CA7C48FD88A5C
A70D0AD4D961DD013D3BBB5BC8E5802B
E4AAF7CF90ED4370E06EC1F6A2B80D9A
BE39A6915BCD6F4E2B3EAC8473243DF1
62547ED8969E6177217D638B211C1A30
457E03C37389A53EA1E500C95D0EFC30
765d27aede93251a79d7685c7403a70b