The FONIX RaaS | New Low-Key Threat with Unnecessary Complexities

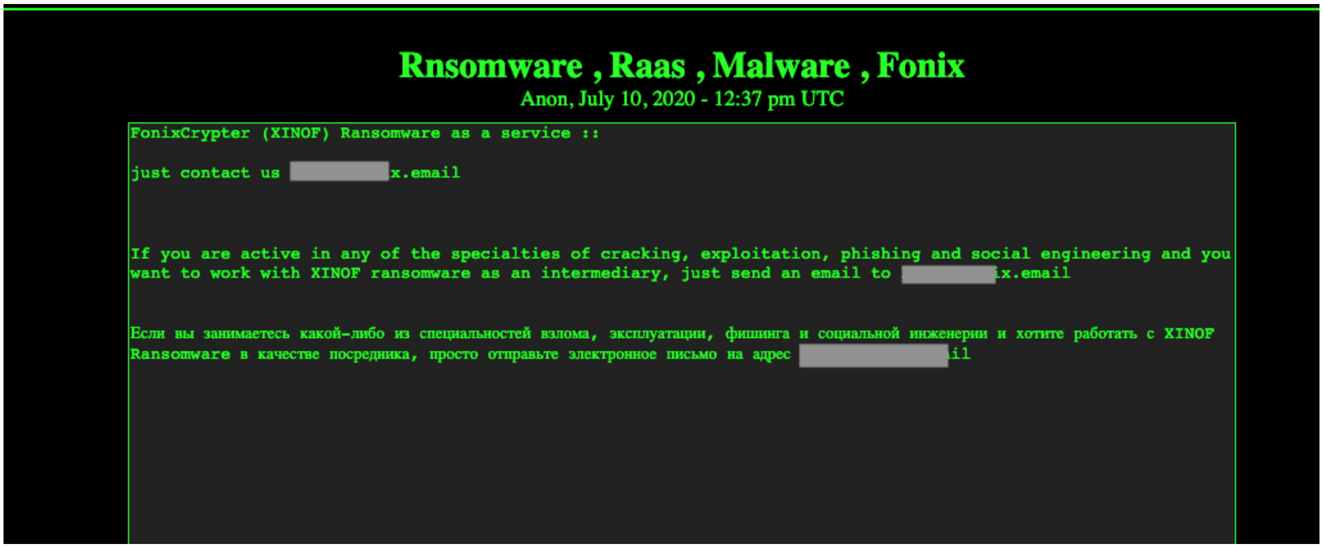
labs.sentinelone.com/the-fonix-raas-new-low-key-threat-with-unnecessary-complexities/

Jim Walter

FONIX Raas (Ransomware as a Service) is an offering that first came to attention in July of this year. It did not make much of a splash at the time, and even currently, we are only seeing small numbers of infections due to this ransomware family. However, RaaS that at first fly under the radar can quickly become rampant if defenders and security solutions remain unaware of them. Notably, FONIX varies somewhat from many other current RaaS offerings in that it employs four methods of encryption for each file and has an overly-complex post-infection engagement cycle. In this post, we dig a little deeper into these and other peculiarities of this new RaaS offering.

FONIX Background: From Crypters to Encrypters

The actors behind FONIX appeared to be primarily focused on binary crypters/packers prior to the release of the RaaS. Their ‘products’ were advertised on various cybercrime forums, as well paste-based advertisements on the Dark Web. Initial advertisement for the RaaS followed suit.



Rnsomware , Raas , Malware , Fonix

Anon, July 10, 2020 - 12:37 pm UTC

```
FonixCrypter (XINOF) Ransomware as a service ::

just contact us [redacted]x.email


If you are active in any of the specialties of cracking, exploitation, phishing and social engineering and you
want to work with XINOF ransomware as an intermediary, just send an email to [redacted]ix.email


Если вы занимаетесь какой-либо из специальностей взлома, эксплуатации, фишинга и социальной инженерии и хотите работать с XINOF
Ransomware в качестве посредника, просто отправьте электронное письмо на адрес [redacted]il
```

FONIX RaaS: A Complex Victim-Affiliate-Author Triangle

Engagement for this RaaS is handled purely via email, and directly with the author/advertiser. There is no web-based portal to register or manage infections or campaigns. The authors did appear to initially offer a FONIX-specific email service; however, at the time of writing, that service appears to be unavailable.

Upon engaging with the FONIX advertiser, would-be buyers are required to supply the malware author with their desired email address and password for the FONIX mail service. Since the FONIX mail service is currently inactive as noted, it appears that buyers are to supply the sellers with alternative email addresses (e.g., protonmail). Once the seller has received the email data, the buyer is sent copies of the ransomware payloads.

The received payloads are customized to display the email address of the new buyer upon infection, which in turn directs the victims to reach out via said email in order to receive decryption instructions, or acquire proof of decryption. Again, all transactions are handled via email, as opposed to a web-based portal.

There is no upfront cost for becoming a FONIX affiliate. Rather, when victims pay their ransom (which they should ideally not do), the attacker (FONIX buyer) provides the FONIX authors with a 25% cut of the proceeds.

The actual process is a bit convoluted and far less user-friendly than most ransomware services. Based on current intelligence, we know that FONIX affiliates do not get provided with a decryptor utility or keys at first. Instead, victims first contact the affiliate (buyer) via email as described above. The affiliate then requests a few files from the victim. These include two small files for decryption: one is to provide proof to the victim, the other is the file “cpriv.key” from the infected host. The affiliate is then required to send those files to the FONIX authors, who decrypt the files, after which they can be sent to the victims.

Presumably, once the victim is satisfied that decryption is possible, the affiliate provides a payment address (BTC wallet). The victim then pays the affiliate, with the affiliate in turn supplying the FONIX authors with their 25% cut.

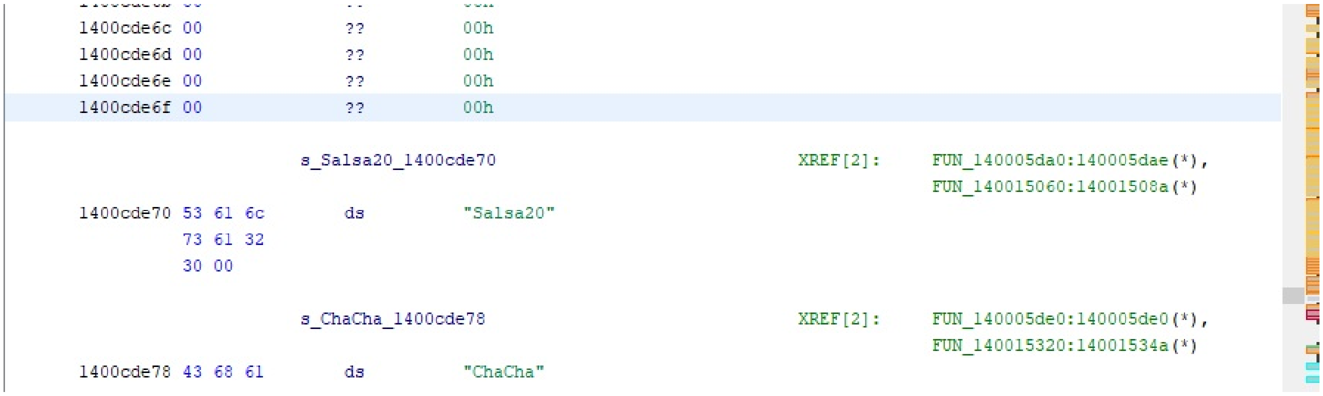
Once the FONIX authors have received their portion of the proceeds, they provide the affiliate with the decryptor utility and key (keys are unique to each campaign). At that point, it is between the affiliate and the victim in terms of how they provide the decryption capabilities.

All in all, this makes for a time-consuming process for any environment, especially large enterprises. Prevention of the infection, avoiding the whole rigmarole, is a far more attractive option!

FONIX Ransomware: File Encryption and Execution

The FONIX samples we have observed come in 64 and 32-bit varieties, and are available for Windows only. By default, FONIX will encrypt all file types, excluding critical Windows OS files.

File encryption is handled via a mixture of Salsa20, Chacha, RSA and AES.



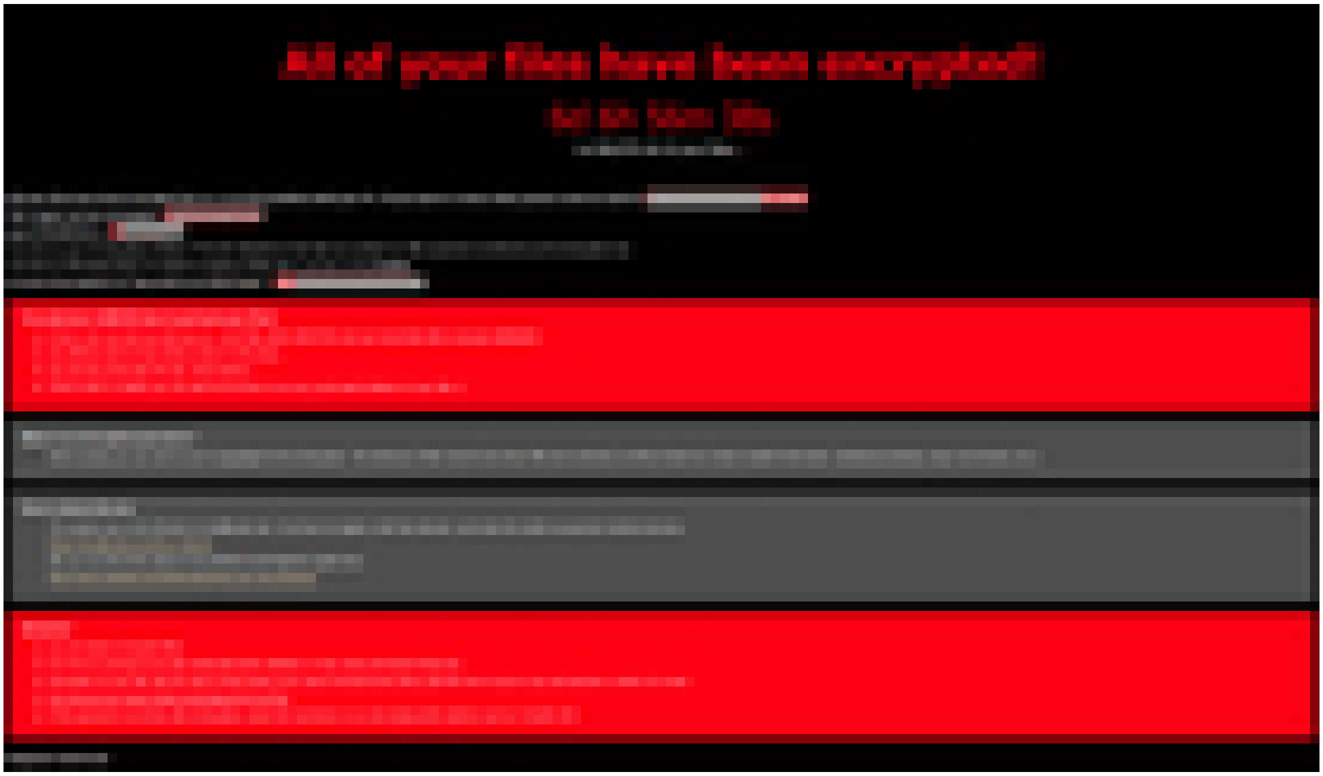
```
     1400cde6c 00          ??        00h
     1400cde6d 00          ??        00h
     1400cde6e 00          ??        00h
     1400cde6f 00          ??        00h

                     s_Salsa20_1400cde70                    XREF[2]:     FUN_140005da0:140005dae(*),
                                                                         FUN_140015060:14001508a(*)
     1400cde70 53 61 6c    ds        "Salsa20"
               73 61 32
               30 00

                     s_ChaCha_1400cde78                     XREF[2]:     FUN_140005de0:140005de0(*),
                                                                         FUN_140015320:14001534a(*)
     1400cde78 43 68 61    ds        "ChaCha"
```

The FONIX authors advertise that this is to ensure “strong” and “unbeatable” encryption. However, this does add considerable time to the encryption process. Our analysis shows that FONIX is between 2 and 5 times slower than other well-known ransomware families (e.g., Ryuk, NetWalker).

Encrypted files are all marked with the `.XINOF` extension (FONIX backwards). Depending on the context of the executed payload, numerous other malicious changes are made to the system. In all cases, once encryption is complete, the Desktop background is changed to the FONIX logo, and the `.HTA` -formatted ransomware note is displayed across the entire screen.

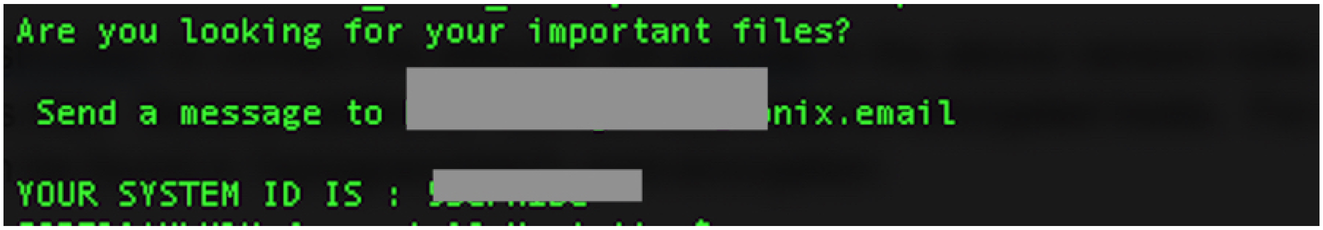


As noted, instructions to contact the attacker are provided in the ransom note (`How To Decrypt Files.hta`). Several additional files are deposited on encrypted hosts. For example, the following can be found in `%programdata%` post-encryption:

- Cpriv.key
- Hello Michaele Gllips

- Help.txt
- How To Decrypt Files.hta
- SystemID

`Cpriv.key` and `SystemID` are both required for decryption, as detailed in the decryption chain process described above. `How To Decrypt Files.hta` is the primary ransom note, and this is the same HTA displayed prominently (covering up the FONIX logo wallpaper however). `Help.txt` is an additional plain text file containing the same attacker email address. The file simply contains a quick message, the attacker email address and the SystemID.

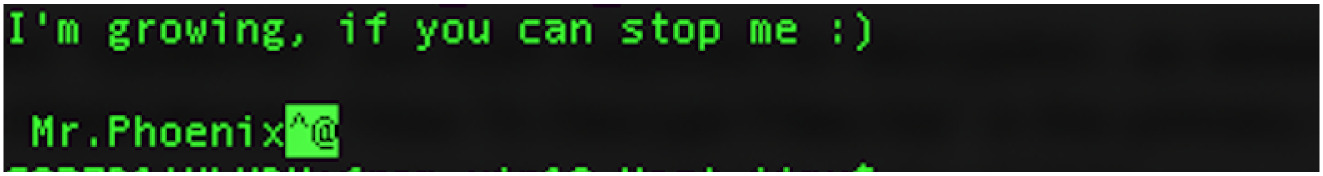


```
Are you looking for your important files?

 Send a message to [redacted]nix.email

YOUR SYSTEM ID IS : [redacted]
```

The remaining file `Hello Michaele Gllips` appears to be a message to @demonslay335 of the MalwareHunterTeam. This was also documented, via Twitter, by @bartblaze.

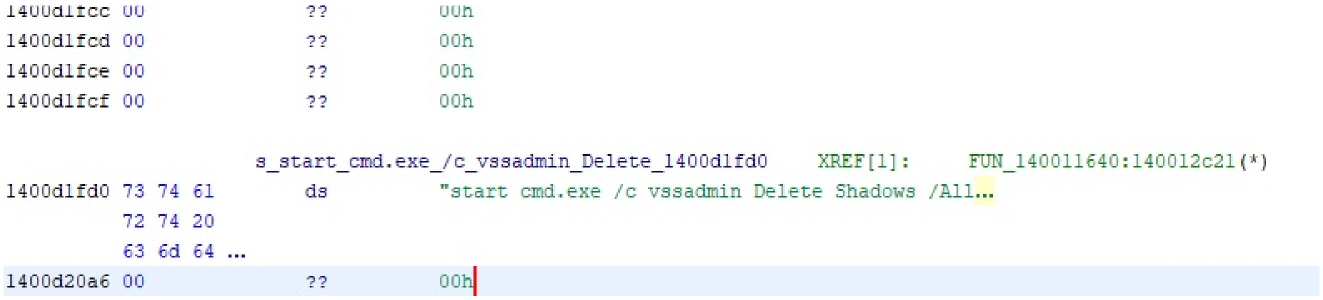


```
I'm growing, if you can stop me :)

 Mr.Phoenix^@
```

When executed with administrator privileges, the following additional system changes occur:

- Task Manager is disabled
- Persistence is achieved via scheduled task, Startup folder inclusion, and the registry (Run AND RunOnce)
- System file permissions are modified
- Persistent copies of the payload have their attributed set to hidden
- A hidden service is created for persistence (Windows 10)
- Drive / Volume labels are changed (to “XINOF”)
- Volume Shadow Copies are deleted (vssadmin, wmic)
- System recovery options are manipulated/disabled (bcdedit)
- Safeboot options are manipulated



```
1400d1fcc 00              ??         00h
1400d1fcd 00              ??         00h
1400d1fce 00              ??         00h
1400d1fcf 00              ??         00h

                s_start_cmd.exe_/c_vssadmin_Delete_1400d1fd0    XREF[1]:     FUN_140011640:140012c21(*)
1400d1fd0 73 74 61        ds         "start cmd.exe /c vssadmin Delete Shadows /All…
          72 74 20
          63 6d 64 …
1400d20a6 00              ??         00h
```

The FONIX malware executes numerous system-altering commands. This is just a small sample of the many we observed:

```
conhost.exe 0xffffffff -ForceV1
cmd.exe /c schtasks /CREATE /SC ONLOGON /TN fonix /TR C:ProgramDataXINOF.exe /RU
SYSTEM /RL HIGHEST /F
schtasks.exe /RU SYSTEM /RL HIGHEST /F
cmd.exe /c copy XINOF.exe %appdata%MicrosoftWindowsStart MenuProgramsStartupXINOF.exe
cmd.exe /c attrib +h +s C:Usersadmin1AppDataRoamingMicrosoftWindowsStart
MenuProgramsStartupXINOF.exe
attrib.exe
cmd.exe /c reg add HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun /v
"PhoenixTechnology" /t REG_SZ /d C:ProgramDataXINOF.exe /f
reg.exe /f
cmd.exe /c reg add HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRun /v
"PhoenixTechnology" /t REG_SZ /d C:ProgramDataXINOF.exe /f
cmd.exe /c reg add HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRunOnce /v
"PhoenixTechnology" /t REG_SZ /d C:ProgramDataXINOF.exe /f
cmd.exe /c reg add HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRunOnce /v
"PhoenixTechnology" /t REG_SZ /d C:ProgramDataXINOF.exe /f
cmd.exe /c reg add
HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionPoliciesSystem   /v
DisableTaskMgr  /t REG_DWORD /d 1 /f
reg.exe add HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionPoliciesSystem
/v DisableTaskMgr  /t REG_DWORD /d 1 /f
cmd.exe /c reg add
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem   /v
DisableTaskMgr  /t REG_DWORD /d 1 /f
```

Conclusion

FONIX is not at present a widespread threat; whether that is due to the complexity of its engagement model or other factors is difficult to say at this time. However, a FONIX infection is notably aggressive – encrypting everything other than system files – and can be difficult to recover from once a device has been fully encrypted. Currently, FONIX does not appear to be threatening victims with additional consequences (such as public data exposure or DDoS attacks) for non-compliance. Even without those extra headaches, however, good user hygiene and strong, modern, endpoint security controls are critical in preventing this and similar infections. The SentinelOne platform is fully able to prevent all behaviors and artifacts associated with the FONIX ransomware family.

Indicators of Compromise

SHA1
a94f92f1e6e4fed57ecb2f4ad55e22809197ba2e
1f551246c5ed70e12371891f0fc6c2149d5fac6b
63cae6a594535e8821c160da4b9a58fc71e46eb2

SHA256
e5324495a9328fe98187239565c05b077680b2ebc9183a6e3e2ccfbfa9f0295a
5263c485f21886aad8737183a71ddc1dc77a92f64c58657c0628374e09bb6899
658ec5aac2290606dba741bce30853515795028322162167395cebc5d0bfccf4

MITRE ATT&CK
Data Encrypted for Impact T1486
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547]Obfuscated Files or Information T1027
Inhibit System Recovery T1490
Scheduled Task/Job: Scheduled Task T1053.005
Boot or Logon Autostart Execution T1547
Command and Scripting Interpreter T1059
Command and Scripting Interpreter: Windows Command Shell T1059.003
Obfuscated Files or Information: Software Packing T1027.002
File and Directory Permissions Modification T1222
File and Directory Permissions Modification: Windows File and Directory Permissions Modification T1222.001
Hide Artifacts T1564
Inhibit System Recovery T1490