iAWACS 2010: W32/ELF/Diffuser

Frédéric Bertrand François-Xavier Bru

MS SSI, Télécom Bretagne & Supélec
{frederic.bertrand, fx.bru}@telecom-bretagne.eu

May 8th, 2010

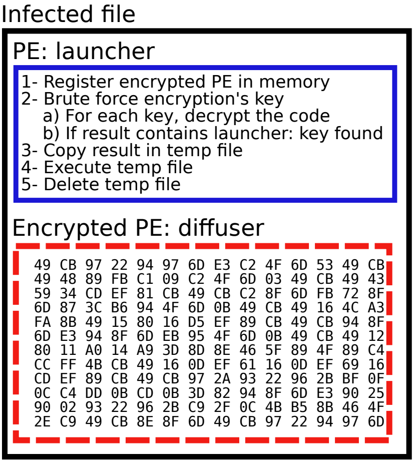
Agenda

1. Main features
2. Launcher
3. Diffuser
4. Questions

Main features

- Type: PE infection
- Payload: user's documents deletion
- Static analysis countermeasure: self-encryption
- Dynamic analysis countermeasure: temporal obfuscation

Launcher 1/6



Infected file

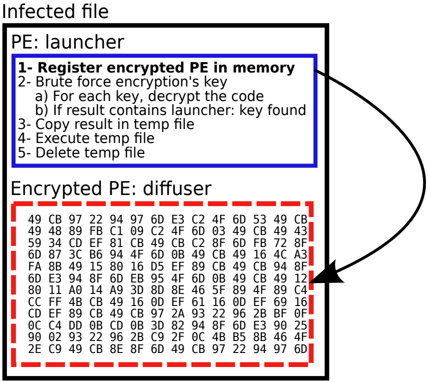
PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
    a) For each key, decrypt the code
    b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Launcher 2/6



Infected file

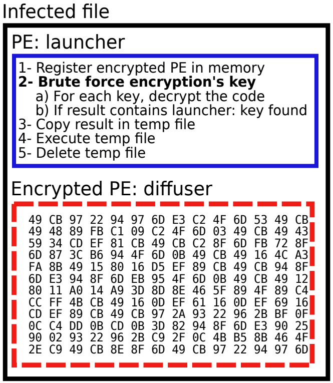
PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
  a) For each key, decrypt the code
  b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Launcher 3/6



Infected file

PE: launcher

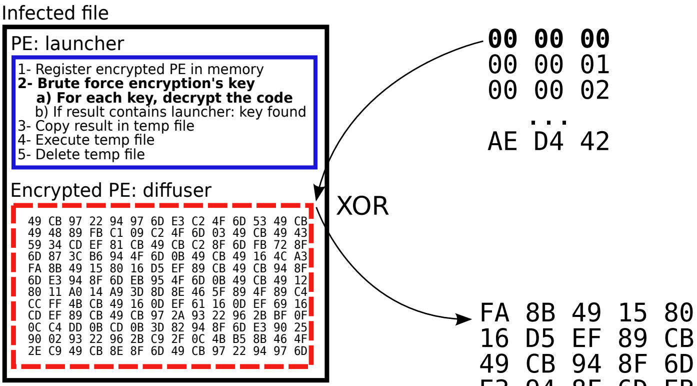
1- Register encrypted PE in memory
2- Brute force encryption's key
 a) For each key, decrypt the code
 b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

```
00 00 00
00 00 01
00 00 02
   ...
AE D4 42
```

Launcher 4/6



Infected file

PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
a) For each key, decrypt the code
b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

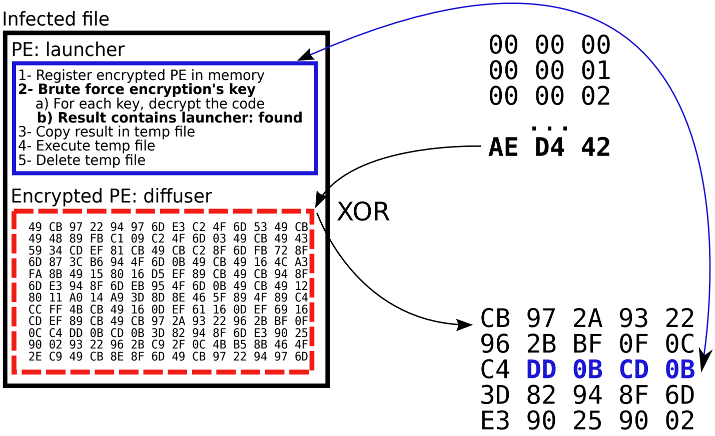
```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

```
00 00 00
00 00 01
00 00 02
  ...
AE D4 42
```

XOR

```
FA 8B 49 15 80
16 D5 EF 89 CB
49 CB 94 8F 6D
E3 94 8F 6D EB
95 4F 6D 0B 49
```

Launcher 5/6



Infected file

PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
a) For each key, decrypt the code
b) Result contains launcher: found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

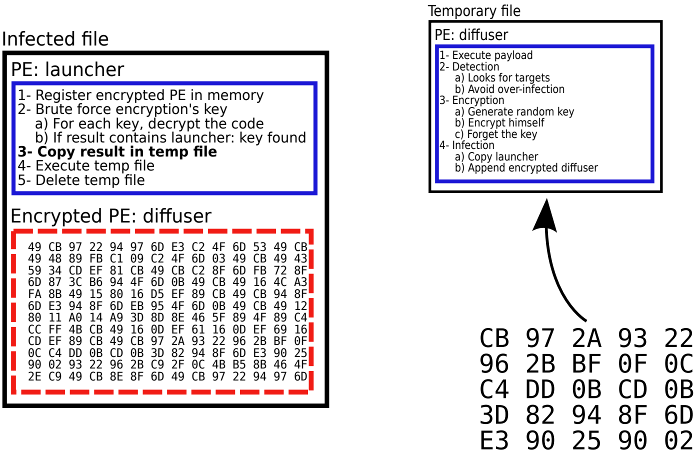
```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

```
00 00 00
00 00 01
00 00 02
   ...
AE D4 42
```

XOR

```
CB 97 2A 93 22
96 2B BF 0F 0C
C4 DD 0B CD 0B
3D 82 94 8F 6D
E3 90 25 90 02
```

Launcher 6/6



Infected file

PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
  a) For each key, decrypt the code
  b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

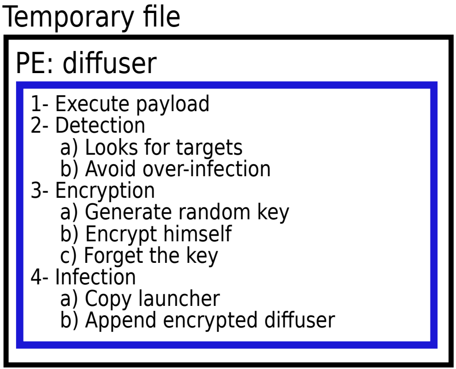
Temporary file

PE: diffuser

1- Execute payload
2- Detection
  a) Looks for targets
  b) Avoid over-infection
3- Encryption
  a) Generate random key
  b) Encrypt himself
  c) Forget the key
4- Infection
  a) Copy launcher
  b) Append encrypted diffuser

```
CB 97 2A 93 22
96 2B BF 0F 0C
C4 DD 0B CD 0B
3D 82 94 8F 6D
E3 90 25 90 02
```

Diffuser 1/13

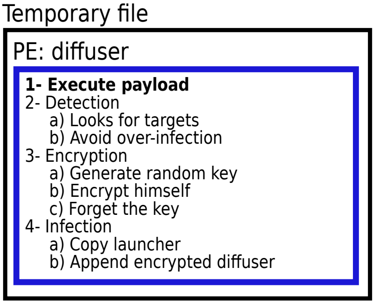


Temporary file

PE: diffuser

1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Diffuser 2/13



Temporary file

PE: diffuser

1- Execute payload
2- Detection
  a) Looks for targets
  b) Avoid over-infection
3- Encryption
  a) Generate random key
  b) Encrypt himself
  c) Forget the key
4- Infection
  a) Copy launcher
  b) Append encrypted diffuser

Diffuser 3/13

Temporary file

PE: diffuser

1- Execute payload
2- Detection
  a) Looks for targets
  b) Avoid over-infection
3- Encryption
  a) Generate random key
  b) Encrypt himself
  c) Forget the key
4- Infection
  a) Copy launcher
  b) Append encrypted diffuser

Diffuser 4/13

Temporary file

PE: diffuser

1- Execute payload

2- Detection

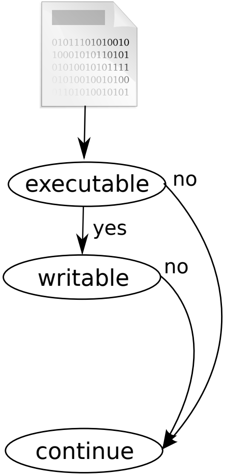
- **a) Looks for targets**
- b) Avoid over-infection

3- Encryption

- a) Generate random key
- b) Encrypt himself
- c) Forget the key

4- Infection

- a) Copy launcher
- b) Append encrypted diffuser



Diffuser 5/13

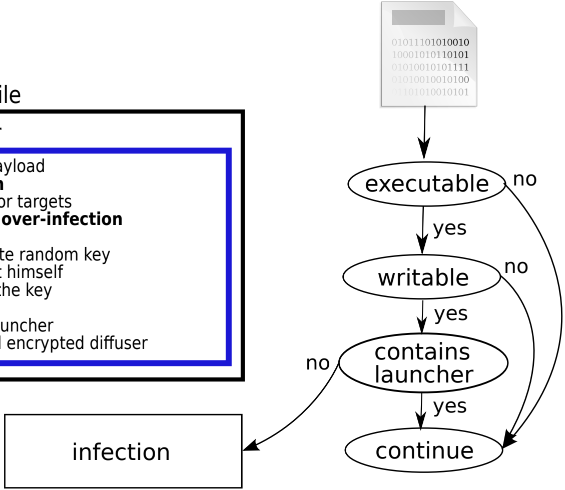
Temporary file

PE: diffuser

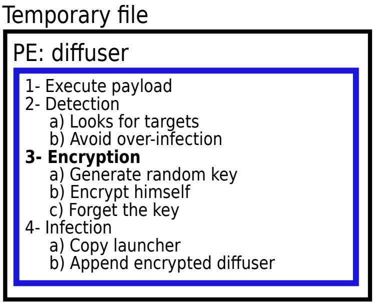
1- Execute payload
2- Detection
- a) Looks for targets
- **b) Avoid over-infection**

3- Encryption
- a) Generate random key
- b) Encrypt himself
- c) Forget the key

4- Infection
- a) Copy launcher
- b) Append encrypted diffuser



Diffuser 6/13



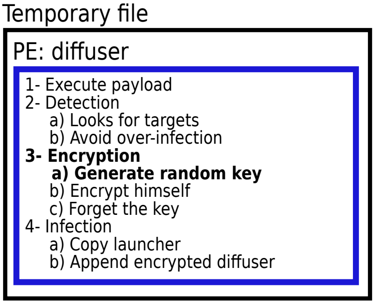
Temporary file

PE: diffuser

1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Diffuser 7/13

AE 42 5D



Temporary file

PE: diffuser

1- Execute payload

2- Detection

a) Looks for targets

b) Avoid over-infection

3- Encryption

a) Generate random key

b) Encrypt himself

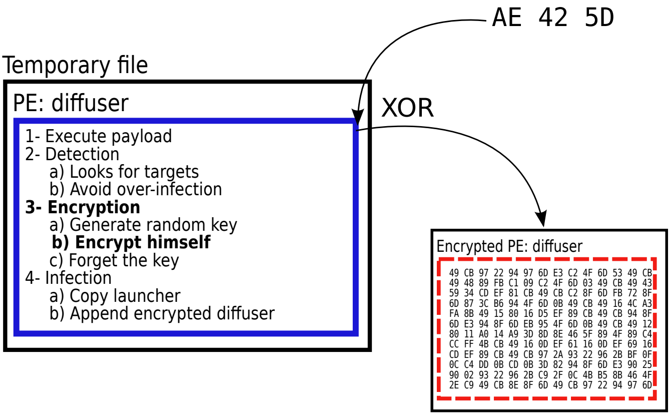
c) Forget the key

4- Infection

a) Copy launcher

b) Append encrypted diffuser

Diffuser 8/13



AE 42 5D

XOR

Temporary file

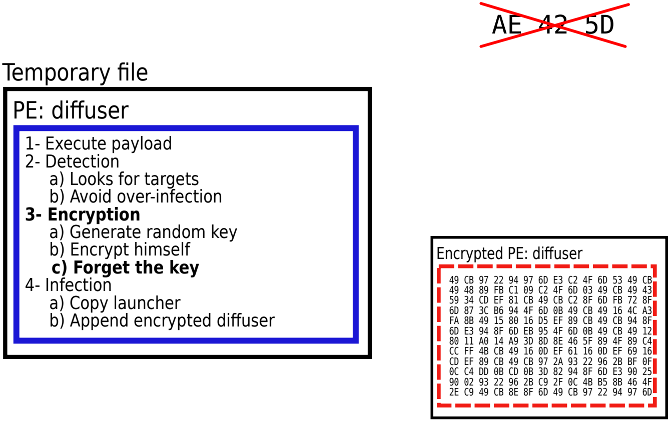
PE: diffuser

1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Diffuser 9/13



~~AE 42 5D~~

Temporary file

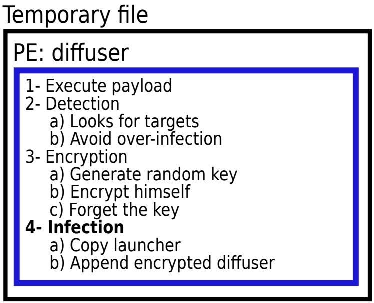
PE: diffuser

1- Execute payload
2- Detection
  a) Looks for targets
  b) Avoid over-infection
3- Encryption
  a) Generate random key
  b) Encrypt himself
  c) Forget the key
4- Infection
  a) Copy launcher
  b) Append encrypted diffuser

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Diffuser 10/13

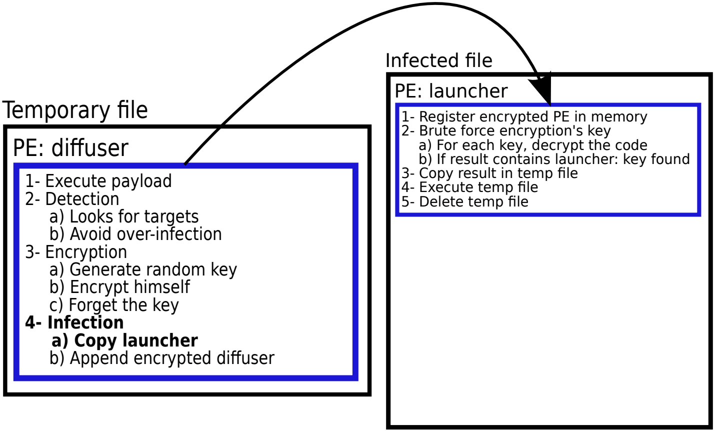


Temporary file

PE: diffuser

1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Diffuser 11/13



Temporary file

PE: diffuser

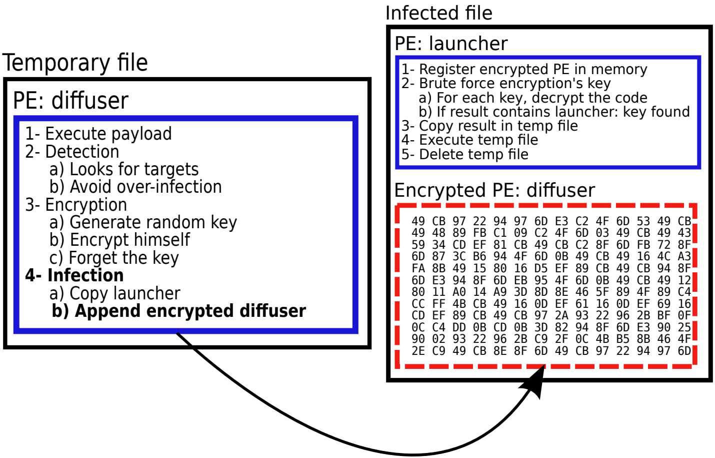
1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Infected file

PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
    a) For each key, decrypt the code
    b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Diffuser 12/13



Temporary file

PE: diffuser

1- Execute payload
2- Detection
    a) Looks for targets
    b) Avoid over-infection
3- Encryption
    a) Generate random key
    b) Encrypt himself
    c) Forget the key
4- Infection
    a) Copy launcher
    b) Append encrypted diffuser

Infected file

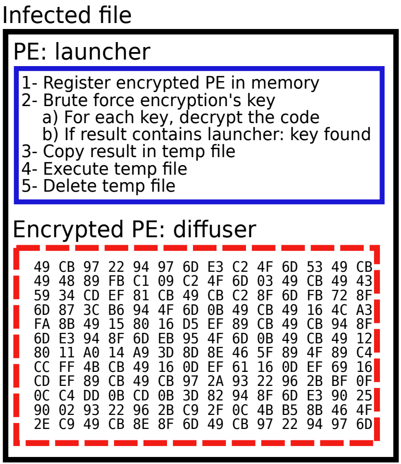
PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
    a) For each key, decrypt the code
    b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Diffuser 13/13



Infected file

PE: launcher

1- Register encrypted PE in memory
2- Brute force encryption's key
    a) For each key, decrypt the code
    b) If result contains launcher: key found
3- Copy result in temp file
4- Execute temp file
5- Delete temp file

Encrypted PE: diffuser

```
49 CB 97 22 94 97 6D E3 C2 4F 6D 53 49 CB
49 48 89 FB C1 09 C2 4F 6D 03 49 CB 49 43
59 34 CD EF 81 CB 49 CB C2 8F 6D FB 72 8F
6D 87 3C B6 94 4F 6D 0B 49 CB 49 16 4C A3
FA 8B 49 15 80 16 D5 EF 89 CB 49 CB 94 8F
6D E3 94 8F 6D EB 95 4F 6D 0B 49 CB 49 12
80 11 A0 14 A9 3D 8D 8E 46 5F 89 4F 89 C4
CC FF 4B CB 49 16 0D EF 61 16 0D EF 69 16
CD EF 89 CB 49 CB 97 2A 93 22 96 2B BF 0F
0C C4 DD 0B CD 0B 3D 82 94 8F 6D E3 90 25
90 02 93 22 96 2B C9 2F 0C 4B B5 8B 46 4F
2E C9 49 CB 8E 8F 6D 49 CB 97 22 94 97 6D
```

Questions

?