

# BAD RABBIT



## Ransomware

Bad Rabbit is a locally self-propagating ransomware, spreading via SMB once inside.

Requires User Interaction

Mostly targeted Russia and the Ukraine.

Primary affected Windows XP thru 7.

```
$ echo -e "\nLance Magnanao \nConstantine Politis \nHenry Lueders" > authors.txt
$ cat authors.txt
```

# What damage was done?

When Bad Rabbit infects a computer; it will distribute or block access to data for ransom.

Individuals that are victimized by this ransomware are directed to a payment site and given 40 hours to pay or the data will be spread across the net; or an increase of ransom for additional time.

Usually the amount would start around 0.05 bitcoins or around \$285 (with the price of bitcoin back then).

`Dops! Your files have been encrypted.`

`If you see this text, your files are no longer accessible.  
You might have been looking for a way to recover your files.  
Don't waste your time. No one will be able to recover them without our  
decryption service.`

`We guarantee that you can recover all your files safely. All you  
need to do is submit the payment and get the decryption password.`

`Visit our web service at caforssztxqzf2nm.onion`

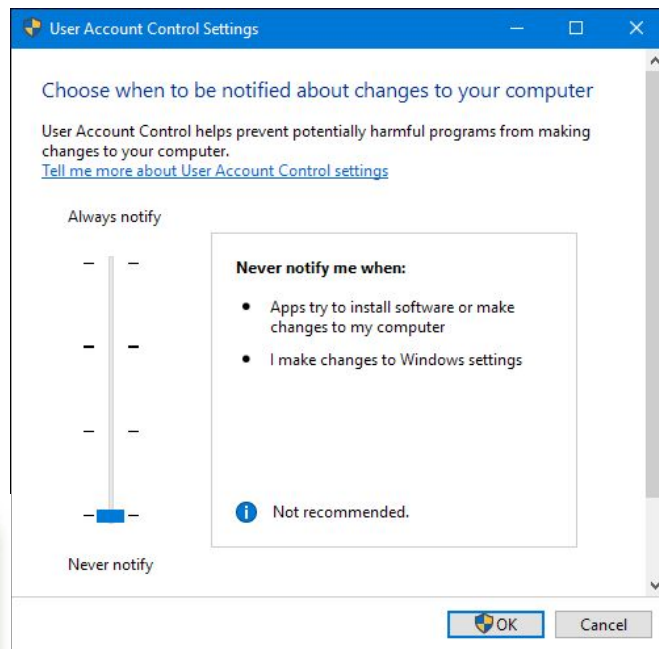
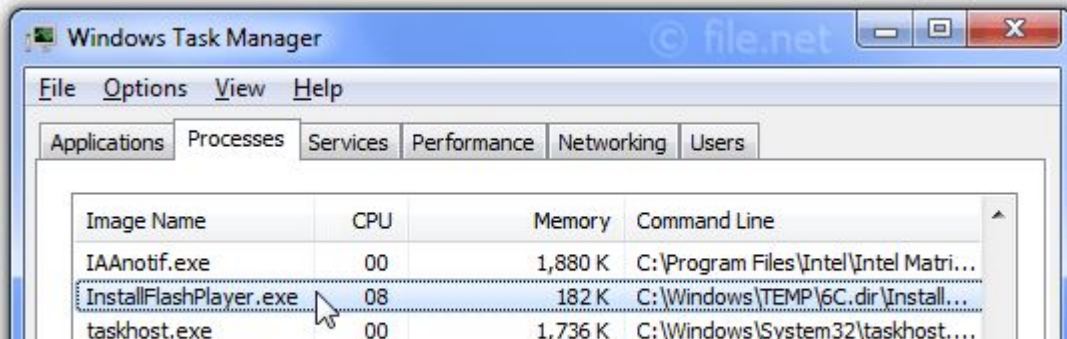
`Your personal installation key#1:`

`2MCOXDgX7oKoxrakfBMXAloe0t6McW7WfX5I+rjJD8hzv6DPpYhNQNCivjW6GX3w  
y4wZX6UdirzbsD7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T301c0ig  
mc1AvUy+r7lX6QcIBZe3il7gqNTblAyKqUK94dANmsI7hQcrC16q2WnxRjH4rF7e  
3sFUVaJW+iwUbY9m+LjnoMqb5zVJzV3yZsj7UCo.j4bWTrM093a9pGuyh058vPY2I  
2LqEcudkJQFSjUmb8FN7E8pSyo2ZF4.j25KRQMSSESNRt6hBBxV0o3Geb15KBEjWIY  
giKdOdaIP5unWM0IJA5GkfccbgTVX77Kjg==`

`If you have already got the password, please enter it below.  
Password#1: _`

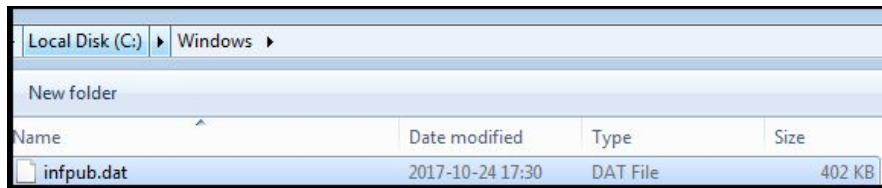
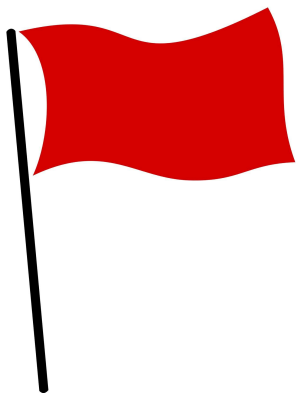
# How was the damage done?

**Bad Rabbit Uses Social Engineering to Infect:** The infection vector starts by visiting a compromised website requesting an Adobe Flash update that downloads the malware. Various reports suggest that the initial infection is caused by compromised web servers that delivered the malicious file (under the name “**install\_flash\_player.exe**”). In order to start the infection, a user will need to download the file from the infected web server and execute it. Depending on User Access Control (UAC) settings, most users will have to accept a popup in order to execute the file. Also, when the user has no admin privileges (high integrity), the malware would not perform malicious actions.



# How was the damage done?

**Installation:** The executable "`install_flash_player.exe`" contains the payload of an encrypted copy of the "`infpub.dat`" file; so, the first stage of the "BadRabbit" malware is to deploy the second stage of the malware:



**Disclaimer: DON'T VISIT THESE SITES!**

## Sample Sites of compromised sites delivering Bad Rabbit:

- Argumentiru[.]com
- fontanka[.]ru
- grupovo[.]bg
- sinematurk[.]com
- aica.co[.]jp
- spbvoditel[.]ru
- argumenti[.]ru
- mediaport[.]ua
- fontanka[.]ru
- an-crimea[.]ru
- t.ks[.]ua
- most-dnepr[.]info
- com[.]ua
- otbrana[.]com
- fontanka[.]ru
- grupovo[.]bg
- pensionhotel[.]cz
- online812[.]ru
- imer[.]ro
- spb[.]ru
- com[.]ua
- pensionhotel[.]com
- ankerch-crimea[.]ru

# How was the damage done?

After the file is dropped, it is executed using `rundll32.exe`. file is created and `"C:\\Windows\\system32\\rundll32.exe C:\\Windows\\infpub.dat,#1 15"` the decrypted data is written to the file.

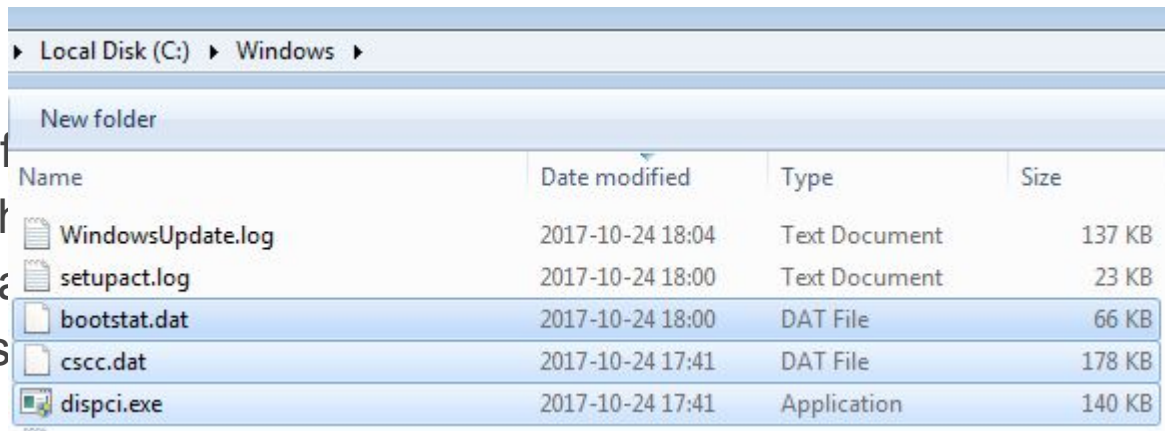
```
00401260 55          push ebp
00401261 56          mov esi, esp
00401262 57          push edi
00401263 58          push esi
00401264 59          push ebx
00401265 5A          push edx
00401266 5B          push ecx
00401267 5C          push eax
00401268 5D          push edi
00401269 5E          push esi
0040126A 5F          push ebx
0040126B 60          push ecx
0040126C 61          push eax
0040126D 62          push edi
0040126E 63          push esi
0040126F 64          push ebx
00401270 65          push ecx
00401271 66          push eax
00401272 67          push edi
00401273 68          push esi
00401274 69          push ebx
00401275 6A          push ecx
00401276 6B          push eax
00401277 6C          push edi
00401278 6D          push esi
00401279 6E          push ebx
0040127A 6F          push ecx
0040127B 70          push eax
0040127C 71          push edi
0040127D 72          push esi
0040127E 73          push ebx
0040127F 74          push ecx
00401280 75          push eax
00401281 76          push edi
00401282 77          push esi
00401283 78          push ebx
00401284 79          push ecx
00401285 7A          push eax
00401286 7B          push edi
00401287 7C          push esi
00401288 7D          push ebx
00401289 7E          push ecx
0040128A 7F          push eax
0040128B 80          push edi
0040128C 81          push esi
0040128D 82          push ebx
0040128E 83          push ecx
0040128F 84          push eax
00401290 85          push edi
00401291 86          push esi
00401292 87          push ebx
00401293 88          push ecx
00401294 89          push eax
00401295 8A          push edi
00401296 8B          push esi
00401297 8C          push ebx
00401298 8D          push ecx
00401299 8E          push eax
0040129A 8F          push edi
0040129B 90          push esi
0040129C 91          push ebx
0040129D 92          push ecx
0040129E 93          push eax
0040129F 94          push edi
004012A0 95          push esi
004012A1 96          push ebx
004012A2 97          push ecx
004012A3 98          push eax
004012A4 99          push edi
004012A5 9A          push esi
004012A6 9B          push ebx
004012A7 9C          push ecx
004012A8 9D          push eax
004012A9 9E          push edi
004012AA 9F          push esi
004012AB A0          push ebx
004012AC A1          push ecx
004012AD A2          push eax
004012AE A3          push edi
004012AF A4          push esi
004012B0 A5          push ebx
004012B1 A6          push ecx
004012B2 A7          push eax
004012B3 A8          push edi
004012B4 A9          push esi
004012B5 AA          push ebx
004012B6 AB          push ecx
004012B7 AC          push eax
004012B8 AD          push edi
004012B9 AE          push esi
004012BA AF          push ebx
004012BB B0          push ecx
004012BC B1          push eax
004012BD B2          push edi
004012BE B3          push esi
004012BF B4          push ebx
004012C0 B5          push ecx
004012C1 B6          push eax
004012C2 B7          push edi
004012C3 B8          push esi
004012C4 B9          push ebx
004012C5 BA          push ecx
004012C6 BB          push eax
004012C7 BC          push edi
004012C8 BD          push esi
004012C9 BE          push ebx
004012CA BF          push ecx
004012CB C0          push eax
004012CC C1          push edi
004012CD C2          push esi
004012CE C3          push ebx
004012CF C4          push ecx
004012D0 C5          push eax
004012D1 C6          push edi
004012D2 C7          push esi
004012D3 C8          push ebx
004012D4 C9          push ecx
004012D5 CA          push eax
004012D6 CB          push edi
004012D7 CC          push esi
004012D8 CD          push ebx
004012D9 CE          push ecx
004012DA CF          push eax
004012DB D0          push edi
004012DC D1          push esi
004012DD D2          push ebx
004012DE D3          push ecx
004012DF D4          push eax
004012E0 D5          push edi
004012E1 D6          push esi
004012E2 D7          push ebx
004012E3 D8          push ecx
004012E4 D9          push eax
004012E5 DA          push edi
004012E6 DB          push esi
004012E7 DC          push ebx
004012E8 DD          push ecx
004012E9 DE          push eax
004012EA DF          push edi
004012EB E0          push esi
004012EC E1          push ebx
004012ED E2          push ecx
004012EE E3          push eax
004012EF E4          push edi
004012F0 E5          push esi
004012F1 E6          push ebx
004012F2 E7          push ecx
004012F3 E8          push eax
004012F4 E9          push edi
004012F5 EA          push esi
004012F6 EB          push ebx
004012F7 EC          push ecx
004012F8 ED          push eax
004012F9 EE          push edi
004012FA EF          push esi
004012FB F0          push ebx
004012FC F1          push ecx
004012FD F2          push eax
004012FE F3          push edi
004012FF F4          push esi
00401300 F5          push ebx
00401301 F6          push ecx
00401302 F7          push eax
00401303 F8          push edi
00401304 F9          push esi
00401305 FA          push ebx
00401306 FB          push ecx
00401307 FC          push eax
00401308 FD          push edi
00401309 FE          push esi
0040130A FF          push ebx
0040130B 00          push ecx
0040130C 01          push eax
0040130D 02          push edi
0040130E 03          push esi
0040130F 04          push ebx
00401310 05          push ecx
00401311 06          push eax
00401312 07          push edi
00401313 08          push esi
00401314 09          push ebx
00401315 0A          push ecx
00401316 0B          push eax
00401317 0C          push edi
00401318 0D          push esi
00401319 0E          push ebx
0040131A 0F          push ecx
0040131B 10          push eax
0040131C 11          push edi
0040131D 12          push esi
0040131E 13          push ebx
0040131F 14          push ecx
00401320 15          push eax
00401321 16          push edi
00401322 17          push esi
00401323 18          push ebx
00401324 19          push ecx
00401325 1A          push eax
00401326 1B          push edi
00401327 1C          push esi
00401328 1D          push ebx
00401329 1E          push ecx
0040132A 1F          push eax
0040132B 20          push edi
0040132C 21          push esi
0040132D 22          push ebx
0040132E 23          push ecx
0040132F 24          push eax
00401330 25          push edi
00401331 26          push esi
00401332 27          push ebx
00401333 28          push ecx
00401334 29          push eax
00401335 2A          push edi
00401336 2B          push esi
00401337 2C          push ebx
00401338 2D          push ecx
00401339 2E          push eax
0040133A 2F          push edi
0040133B 30          push esi
0040133C 31          push ebx
0040133D 32          push ecx
0040133E 33          push eax
0040133F 34          push edi
00401340 35          push esi
00401341 36          push ebx
00401342 37          push ecx
00401343 38          push eax
00401344 39          push edi
00401345 3A          push esi
00401346 3B          push ebx
00401347 3C          push ecx
00401348 3D          push eax
00401349 3E          push edi
0040134A 3F          push esi
0040134B 40          push ebx
0040134C 41          push ecx
0040134D 42          push eax
0040134E 43          push edi
0040134F 44          push esi
00401350 45          push ebx
00401351 46          push ecx
00401352 47          push eax
00401353 48          push edi
00401354 49          push esi
00401355 4A          push ebx
00401356 4B          push ecx
00401357 4C          push eax
00401358 4D          push edi
00401359 4E          push esi
0040135A 4F          push ebx
0040135B 50          push ecx
0040135C 51          push eax
0040135D 52          push edi
0040135E 53          push esi
0040135F 54          push ebx
00401360 55          push ecx
00401361 56          push eax
00401362 57          push edi
00401363 58          push esi
00401364 59          push ebx
00401365 5A          push ecx
00401366 5B          push eax
00401367 5C          push edi
00401368 5D          push esi
00401369 5E          push ebx
0040136A 5F          push ecx
0040136B 60          push eax
0040136C 61          push edi
0040136D 62          push esi
0040136E 63          push ebx
0040136F 64          push ecx
00401370 65          push eax
00401371 66          push edi
00401372 67          push esi
00401373 68          push ebx
00401374 69          push ecx
00401375 6A          push eax
00401376 6B          push edi
00401377 6C          push esi
00401378 6D          push ebx
00401379 6E          push ecx
0040137A 6F          push eax
0040137B 70          push edi
0040137C 71          push esi
0040137D 72          push ebx
0040137E 73          push ecx
0040137F 74          push eax
00401380 75          push edi
00401381 76          push esi
00401382 77          push ebx
00401383 78          push ecx
00401384 79          push eax
00401385 7A          push edi
00401386 7B          push esi
00401387 7C          push ebx
00401388 7D          push ecx
00401389 7E          push eax
0040138A 7F          push edi
0040138B 80          push esi
0040138C 81          push ebx
0040138D 82          push ecx
0040138E 83          push eax
0040138F 84          push edi
00401390 85          push esi
00401391 86          push ebx
00401392 87          push ecx
00401393 88          push eax
00401394 89          push edi
00401395 8A          push esi
00401396 8B          push ebx
00401397 8C          push ecx
00401398 8D          push eax
00401399 8E          push edi
0040139A 8F          push esi
0040139B 90          push ebx
0040139C 91          push ecx
0040139D 92          push eax
0040139E 93          push edi
0040139F 94          push esi
004013A0 95          push ebx
004013A1 96          push ecx
004013A2 97          push eax
004013A3 98          push edi
004013A4 99          push esi
004013A5 9A          push ebx
004013A6 9B          push ecx
004013A7 9C          push eax
004013A8 9D          push edi
004013A9 9E          push esi
004013AA 9F          push ebx
004013AB A0          push ecx
004013AC A1          push eax
004013AD A2          push edi
004013AE A3          push esi
004013AF A4          push ebx
004013B0 A5          push ecx
004013B1 A6          push eax
004013B2 A7          push edi
004013B3 A8          push esi
004013B4 A9          push ebx
004013B5 AA          push ecx
004013B6 AB          push eax
004013B7 AC          push edi
004013B8 AD          push esi
004013B9 AE          push ebx
004013BA AF          push ecx
004013BB B0          push eax
004013BC B1          push edi
004013BD B2          push esi
004013BE B3          push ebx
004013BF B4          push ecx
004013C0 B5          push eax
004013C1 B6          push edi
004013C2 B7          push esi
004013C3 B8          push ebx
004013C4 B9          push ecx
004013C5 BA          push eax
004013C6 BB          push edi
004013C7 BC          push esi
004013C8 BD          push ebx
004013C9 BE          push ecx
004013CA BF          push eax
004013CB C0          push edi
004013CC C1          push esi
004013CD C2          push ebx
004013CE C3          push ecx
004013CF C4          push eax
004013D0 C5          push edi
004013D1 C6          push esi
004013D2 C7          push ebx
004013D3 C8          push ecx
004013D4 C9          push eax
004013D5 CA          push edi
004013D6 CB          push esi
004013D7 CC          push ebx
004013D8 CD          push ecx
004013D9 CE          push eax
004013DA CF          push edi
004013DB D0          push esi
004013DC D1          push ebx
004013DD D2          push ecx
004013DE D3          push eax
004013DF D4          push edi
004013E0 D5          push esi
004013E1 D6          push ebx
004013E2 D7          push ecx
004013E3 D8          push eax
004013E4 D9          push edi
004013E5 DA          push esi
004013E6 DB          push ebx
004013E7 DC          push ecx
004013E8 DE          push eax
004013E9 DF          push edi
004013EA E0          push esi
004013EB E1          push ebx
004013EC E2          push ecx
004013ED E3          push eax
004013EE E4          push edi
004013EF E5          push esi
004013F0 E6          push ebx
004013F1 E7          push ecx
004013F2 E8          push eax
004013F3 E9          push edi
004013F4 EA          push esi
004013F5 EB          push ebx
004013F6 EC          push ecx
004013F7 ED          push eax
004013F8 EE          push edi
004013F9 EF          push esi
004013FA F0          push ebx
004013FB F1          push ecx
004013FC F2          push eax
004013FD F3          push edi
004013FE F4          push esi
004013FF F5          push ebx
00401400 F6          push ecx
00401401 F7          push eax
00401402 F8          push edi
00401403 F9          push esi
00401404 FA          push ebx
00401405 FB          push ecx
00401406 FC          push eax
00401407 FD          push edi
00401408 FE          push esi
00401409 FF          push ebx
0040140A 00          push ecx
0040140B 01          push eax
0040140C 02          push edi
0040140D 03          push esi
0040140E 04          push ebx
0040140F 05          push ecx
00401410 06          push eax
00401411 07          push edi
00401412 08          push esi
00401413 09          push ebx
00401414 0A          push ecx
00401415 0B          push eax
00401416 0C          push edi
00401417 0D          push esi
00401418 0E          push ebx
00401419 0F          push ecx
0040141A 10          push eax
0040141B 11          push edi
0040141C 12          push esi
0040141D 13          push ebx
0040141E 14          push ecx
0040141F 15          push eax
00401420 16          push edi
00401421 17          push esi
00401422 18          push ebx
00401423 19          push ecx
00401424 1A          push eax
00401425 1B          push edi
00401426 1C          push esi
00401427 1D          push ebx
00401428 1E          push ecx
00401429 1F          push eax
0040142A 20          push edi
0040142B 21          push esi
0040142C 22          push ebx
0040142D 23          push ecx
0040142E 24          push eax
0040142F 25          push edi
00401430 26          push esi
00401431 27          push ebx
00401432 28          push ecx
00401433 29          push eax
00401434 2A          push edi
00401435 2B          push esi
00401436 2C          push ebx
00401437 2D          push ecx
00401438 2E          push eax
00401439 2F          push edi
0040143A 30          push esi
0040143B 31          push ebx
0040143C 32          push ecx
0040143D 33          push eax
0040143E 34          push edi
0040143F 35          push esi
00401440 36          push ebx
00401441 37          push ecx
00401442 38          push eax
00401443 39          push edi
00401444 3A          push esi
00401445 3B          push ebx
00401446 3C          push ecx
00401447 3D          push eax
00401448 3E          push edi
00401449 3F          push esi
0040144A 40          push ebx
0040144B 41          push ecx
0040144C 42          push eax
0040144D 43          push edi
0040144E 44          push esi
0040144F 45          push ebx
00401450 46          push ecx
00401451 47          push eax
00401452 48          push edi
00401453 49          push esi
00401454 4A          push ebx
00401455 4B          push ecx
00401456 4C          push eax
00401457 4D          push edi
00401458 4E          push esi
00401459 4F          push ebx
0040145A 50          push ecx
0040145B 51          push eax
0040145C 52          push edi
0040145D 53          push esi
0040145E 54          push ebx
0040145F 55          push ecx
00401460 56          push eax
00401461 57          push edi
00401462 58          push esi
00401463 59          push ebx
00401464 5A          push ecx
00401465 5B          push eax
00401466 5C          push edi
00401467 5D          push esi
00401468 5E          push ebx
00401469 5F          push ecx
0040146A 60          push eax
0040146B 61          push edi
0040146C 62          push esi
0040146D 63          push ebx
0040146E 64          push ecx
0040146F 65          push eax
00401470 66          push edi
00401471 67          push esi
00401472 68          push ebx
00401473 69          push ecx
00401474 6A          push eax
00401475 6B          push edi
00401476 6C          push esi
00401477 6D          push ebx
00401478 6E          push ecx
00401479 6F          push eax
0040147A 70          push edi
0040147B 71          push esi
0040147C 72          push ebx
0040147D 73          push ecx
0040147E 74          push eax
0040147F 75          push edi
00401480 76          push esi
00401481 77          push ebx
00401482 78          push ecx
00401483 79          push eax
00401484 7A          push edi
00401485 7B          push esi
00401486 7C          push ebx
00401487 7D          push ecx
00401488 7E          push eax
00401489 7F          push edi
0040148A 80          push esi
0040148B 81          push ebx
0040148C 82          push ecx
0040148D 83          push eax
0040148E 84          push edi
0040148F 85          push esi
00401490 86          push ebx
00401491 87          push ecx
00401492 88          push eax
00401493 89          push edi
00401494 8A          push esi
00401495 8B          push ebx
00401496 8C          push ecx
00401497 8D          push eax
00401498 8E          push edi
00401499 8F          push esi
0040149A 90          push ebx
0040149B 91          push ecx
0040149C 92          push eax
0040149D 93          push edi
0040149E 94          push esi
0040149F 95          push ebx
004014A0 96          push ecx
004014A1 97          push eax
004014A2 98          push edi
004014A3 99          push esi
004014A4 9A          push ebx
004014A5 9B          push ecx
004014A6 9C          push eax
004014A7 9D          push edi
004014A8 9E          push esi
004014A9 9F          push ebx
004014AA A0          push ecx
004014AB A1          push eax
004014AC A2          push edi
004014AD A3          push esi
004014AE A4          push ebx
004014AF A5          push ecx
004014B0 A6          push eax
004014B1 A7          push edi
004014B2 A8          push esi
004014B3 A9          push ebx
004014B4 AA          push ecx
004014B5 AB          push eax
004014B6 AC          push edi
004014B7 AD          push esi
004014B8 AE          push ebx
004014B9 AF          push ecx
004014BA B0          push eax
004014BB B1          push edi
004014BC B2          push esi
004014BD B3          push ebx
004014BE B4          push ecx
004014BF B5          push eax
004014C0 B6          push edi
004014C1 B7          push esi
004014C2 B8          push ebx
004014C3 B9          push ecx
004014C4 BA          push eax
004014C5 BB          push edi
004014C6 BC          push esi
004014C7 BD          push ebx
004014C8 BE          push ecx
004014C9 BF          push eax
004014CA C0          push edi
004014CB C1          push esi
004014CC C2          push ebx
004014CD C3          push ecx
004014CE C4          push eax
004014CF C5          push edi
004014D0 C6          push esi
004014D1 C7          push ebx
004014D2 C8          push ecx
004014D3 C9          push eax
004014D4 CA          push edi
004014D5 CB          push esi
004014D6 CC          push ebx
004014D7 CD          push ecx
004014D8 CE          push eax
004014D9 CF          push edi
004014DA D0          push esi
004014DB D1          push ebx
004014DC D2          push ecx
004014DD D3          push eax
004014DE D4          push edi
004014DF D5          push esi
004014E0 D6          push ebx
004014E1 D7          push ecx
004014E2 D8          push eax
004014E3 D9          push edi
004014E4 DA          push esi
004014E5 DB          push ebx
004014E6 DC          push ecx
004014E7 DE          push eax
004014E8 DF          push edi
004014E9 EA          push esi
004014EA EB          push ebx
004014EB EC          push ecx
004014EC ED          push eax
004014ED EE          push edi
004014EE EF          push esi
004014EF F0          push ebx
004014F0 F1          push ecx
004014F1 F2          push eax
004014F2 F3          push edi
004014F3 F4          push esi
004014F4 F5          push ebx
004014F5 F6          push ecx
004014F6 F7          push eax
004014F7 F8          push edi
004014F8 F9          push esi
004014F9 FA          push ebx
004014FA FB          push ecx
004014FB FC          push eax
004014FC FD          push edi
004014FD FE          push esi
004014FE FF          push ebx
004014FF 00          push ecx
00401500 01          push eax
00401501 02          push edi
00401502 03          push esi
00401503 04          push ebx
00401504 05          push ecx
00401505 06          push eax
00401506 07          push edi
00401507 08          push esi
00401508 09          push ebx
00401509 0A          push ecx
0040150A 0B          push eax
0040150B 0C          push edi
0040150C 0D          push esi
0040150D 0E          push ebx
0040150E 0F          push ecx
0040150F 10          push eax
00401510 11          push edi
00401511 12          push esi
00401512 13          push ebx
00401513 14          push ecx
00401514 15          push eax
00401515 16          push edi
00401516 17          push esi
00401517 18          push ebx
00401518 19          push ecx
00401519 1A          push eax
0040151A 1B          push edi
0040151B 1C          push esi
0040151C 1D          push ebx
0040151D 1E          push ecx
0040151E 1F          push eax
0040151F 20          push edi
00401520 21          push esi
00401521 22          push ebx
00401522 23          push ecx
00401523 24          push eax
00401524 25          push edi
00401525 26          push esi
00401526 27          push ebx
00401527 28          push ecx
00401528 29          push eax
00401529 2A          push edi
0040152A 2B          push esi
0040152B 2C          push ebx
0040152C 2D          push ecx
0040152D 2E          push eax
0040152E 2F          push edi
0040152F 30          push esi
00401530 31          push ebx
00401531 32          push ecx
00401532 33          push eax
00401533 34          push edi
00401534 35          push esi
00401535 36          push ebx
00401536 37          push ecx
00401537 38          push eax
00401538 39          push edi
00401539 3A          push esi
0040153A 3B          push ebx
0040153B 3C          push ecx
0040153C 3D          push eax
0040153D 3E          push edi
0040153E 3F          push esi
0040153F 40          push ebx
00401540 41          push ecx
00401541 42          push eax
00401542 43          push edi
00401543 44          push esi
00401544 45          push ebx
00401545 46          push ecx
00401546 47          push eax
00401547 48          push edi
00401548 49          push esi
00401549 4A          push ebx
0040154A 4B          push ecx
0040154B 4C          push eax
0040154C 4D          push edi
0040154D 4E          push esi
0040154E 4F          push ebx
0040154F 50          push ecx
00401550 51          push eax
00401551 52          push edi
00401552 53          push esi
00401553 54          push ebx
00401554 55          push ecx
00401555 56          push eax
00401556 57          push edi
00401557 58          push esi
00401558 59          push ebx
00401559 5A          push ecx
0040155A 5B          push eax
0040155B 5C          push edi
0040155C 5D          push esi
0040155D 5E          push ebx
0040155E 5F          push ecx
0040155F 60          push eax
00401560 61          push edi
00401561 62          push esi
00401562 63          push ebx
00401563 64          push ecx
00401564 65          push eax
00401565 66          push edi
00401566 67          push esi
00401567 68          push ebx
00401568 69          push ecx
00401569 6A          push eax
0040156A 6B          push edi
0040156B 6C          push esi
0040156C 6D          push ebx
0040156D 6E          push ecx
0040156E 6F          push eax
0040156F 70          push edi
00401570 71          push esi
00401571 72          push ebx
00401572 73          push ecx
00401573 74          push eax
00401574 75          push edi
00401575 76          push esi
00401576 77          push ebx
00401577 78          push ecx
00401578 79          push eax
00401579 7A          push edi
0040157A 7B          push esi
0040157B 7C          push ebx
0040157C 7D          push ecx
0040157D 7E          push eax
0040157E 7F          push edi
0040157F 80          push esi
00401580 81          push ebx
00401581 82          push ecx
00401582 83          push eax
00401583 84          push edi
00401584 85          push esi
00401585 86          push ebx
00401586 87          push ecx
00401587 88          push eax
00401588 89          push edi
00401589 8A          push esi
0040158A 8B          push ebx
0040158B 8C          push ecx
0040158C 8D          push eax
0040158D 8E          push edi
0040158E 8F          push esi
0040158F 90          push ebx
00401590 91          push ecx
00401591 92          push eax
00401592 93          push edi
00401593 94          push esi
00401594 95          push ebx
00401595 96          push ecx
00401596 97          push eax
00401597 98          push edi
00401598 99          push esi
00401599 9A          push ebx
0040159A 9B          push ecx
0040159B 9C          push eax
0040159C 9D          push edi
0040159D 9E          push esi
0040159E 9F          push ebx
0040159F A0          push ecx
004015A0 A1          push eax
004015A1 A2          push edi
004015A2 A3          push esi
004015A3 A4          push ebx
004015A4 A5          push ecx
004015A5 A6          push eax
004015A6 A7          push edi
004015A7 A8          push esi
004015A8 A9          push ebx
004015A9 AA          push ecx
004015AA AB          push eax
004015AB AC          push edi
004015AC AD          push esi
004015AD AE          push ebx
004015AE AF          push ecx
004015AF B0          push eax
004015B0 B1          push edi

```

# How was the damage done?

“**infpub.dat**”

the malicious f  
familiar from th  
most of the ma  
additional files



Name	Date modified	Type	Size
WindowsUpdate.log	2017-10-24 18:04	Text Document	137 KB
setupact.log	2017-10-24 18:00	Text Document	23 KB
bootstat.dat	2017-10-24 18:00	DAT File	66 KB
cscd.dat	2017-10-24 17:41	DAT File	178 KB
dispcpi.exe	2017-10-24 17:41	Application	140 KB

er portion of  
ension is  
) to perform  
rops three

- “C:\Windows\cscd.dat” - **cscd.dat** – legitimate driver used for the disk encryption ([diskcryptor.net](http://diskcryptor.net))
- “C:\Windows\dispcpi.exe” - **dispcpi.exe** – installs the bootlocker, communicates with the driver
- “C:\Windows\<random-name>.tmp” - mimikatz binary used for obtaining passwords

# How was the damage done?

First, the malware enables privileges using `AdjustTokenPrivileges()`.

**The malware enables the following privileges:**

- “`SeShutdownPrivilege`” - gives the ability to shut down local system.
- “`SeDebugPrivilege`” - gives the ability to debug.
- “`SeTcbPrivilege`” - its holder is recognized as part of the trusted computer base.

```
esi          ; ReturnLength
esi          ; PreviousState
esi          ; BufferLength
eax, [ebp+NewState]
eax          ; NewState
esi          ; DisableAllPrivileges
[ebp+TokenHandle] ; TokenHandle
[ebp+NewState.PrivilegeCount], 1
[ebp+NewState.Privileges.Attributes], 2
ds:AdjustTokenPrivileges
```



# How was the damage done?

Next, the malware drops additional files. The first is "cscce.dat" that will

b  
e

```
push    offset pMore      ; "dispci.exe"
lea     eax, [ebp+pszPath]
push    eax               ; pszPath
call    ds:PathAppendW
test    eax, eax
jz      short loc_100011D7
```

```
push    [ebp+lpMem]
mov     ebx, [ebp+var_8]
lea     eax, [ebp+pszPath]
push    eax
call    r_CreatesNewFile
```

```
10007E8E sub_10007E8E proc near
10007E8E
10007E8E pszDest= word ptr -620h
10007E8E var_8= dword ptr -8
10007E8E var_4= dword ptr -4
10007E8E push    esi
10007E8F mov     esi, esp
10007E91 sub     esp, 620h
10007E97 push    esi
10007E98 lea     eax, [ebp+var_8]
10007E9E push    eax
10007E9F xor     esi, esi
10007EA1 call    sub_10007E8E
10007EA6 test    eax, eax
10007EA8 jz      short loc_10007EFC
```

If "cscce.dat" does not exist it is created. If "cscce.dat" already exists the malware terminates. Next, the "dispci.exe" file is created. Its main purpose is to perform part of the encryption and the decryption using "DiskCryptor" driver utilities.

```
10007E8A lea     eax, [ebp+pszDest]
10007E8B push    eax               ; pszPath
10007E8C call    ds:PathFileExistsW
10007E8E test    eax, eax
10007E8F jnz     short loc_10007EFC
```

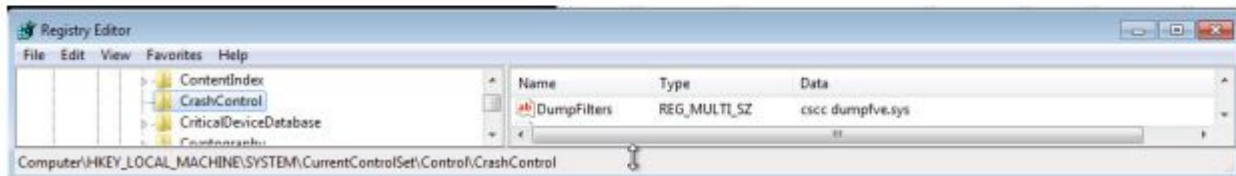
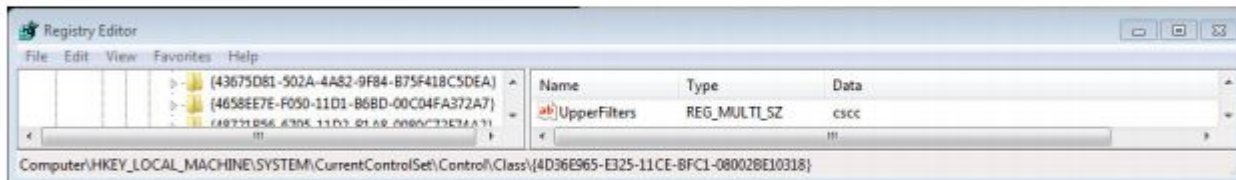
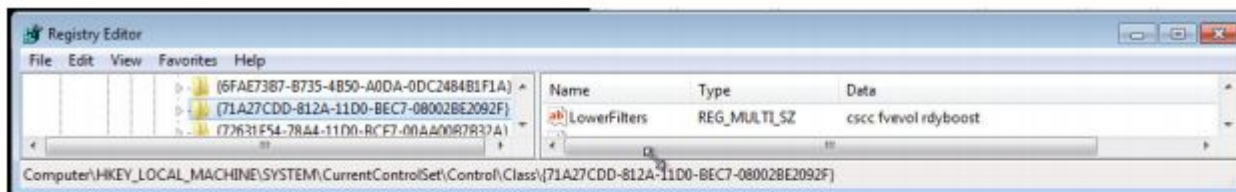
```
10007EFC loc_10007EFC:                ; uExitCode
10007EFC push    esi
10007EFD call    ds:ExitProcess
10007EFD sub_10007E8E endp
10007EFD
```



# How was the damage done?

Registering 'cscd.dat' as a Service In "Order Filters", "UpperFilters" and "DumpFilters" service as a driver under the name "cscd" are added.

Then the main  
following reg  
Key: "HKEY\_  
SYSTEMC  
vices\cdfs"

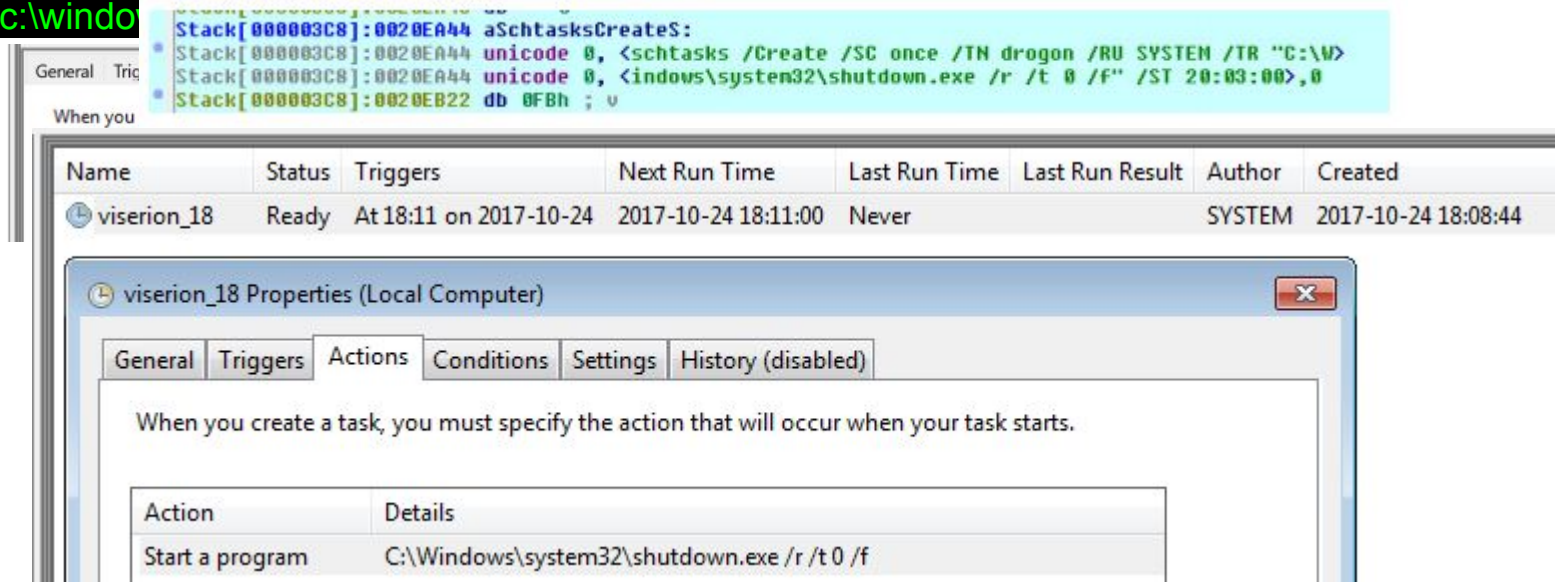


# How was the damage done?

After the driver is registered, the malware adds two new scheduled tasks:

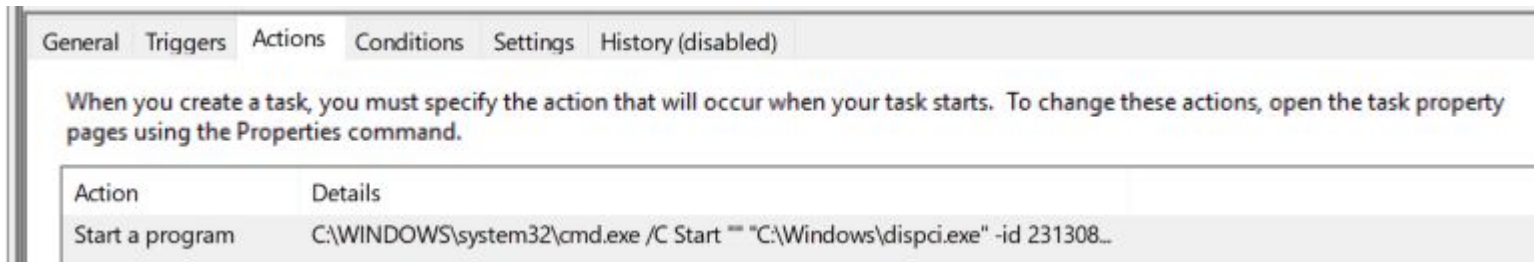
1. The first scheduled task is added with the purpose of affecting boot on the `dispci.exe` `cmd.exe`
2. The second scheduled task is added with the purpose of affecting boot on the `dispci.exe` `cmd.exe`

The scheduled task is set using the `/c schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "C:\Windows\system32\shutdown.exe /r /t 0 /f /ST 'EM /SC ONSTART /TN rhaegal / TR "c:\windo`



# How was the damage done?

**File Encryption Process:** The dropped application “**dispci.exe**” (DiskCryptor) is run with the help of one of the scheduled task:



The malware encrypts files with the selected extensions. All the files are encrypted with the same key (the same plaintext gives the same ciphertext).

```
3ds 7z accdb ai asm asp aspx avhd back bak bmp brw c cab
cc cer cfg conf cpp crt cs ctl cxx dbf der dib disk djvu
doc docx dwg eml fdb gz h hdd hpp hxx iso java jfif jpe
jpeg jpg js kdbx key mail mdb msg nrg odc odf odg odi odm
odp ods odt ora ost ova ovf p12 p7b p7c pdf pem pfx php
pmf png ppt pptx ps1 pst pvi py pyc pyw qcow qcow2 rar rb
rtf scm sln sql tar tib tif tiff vb vbox vbs vcb vdi vfd
vhd vhdx vmc vmdk vmsd vmtm vmx vsdx vsv work xls xlsx x
ml xvd zip
```

# How was the damage done?

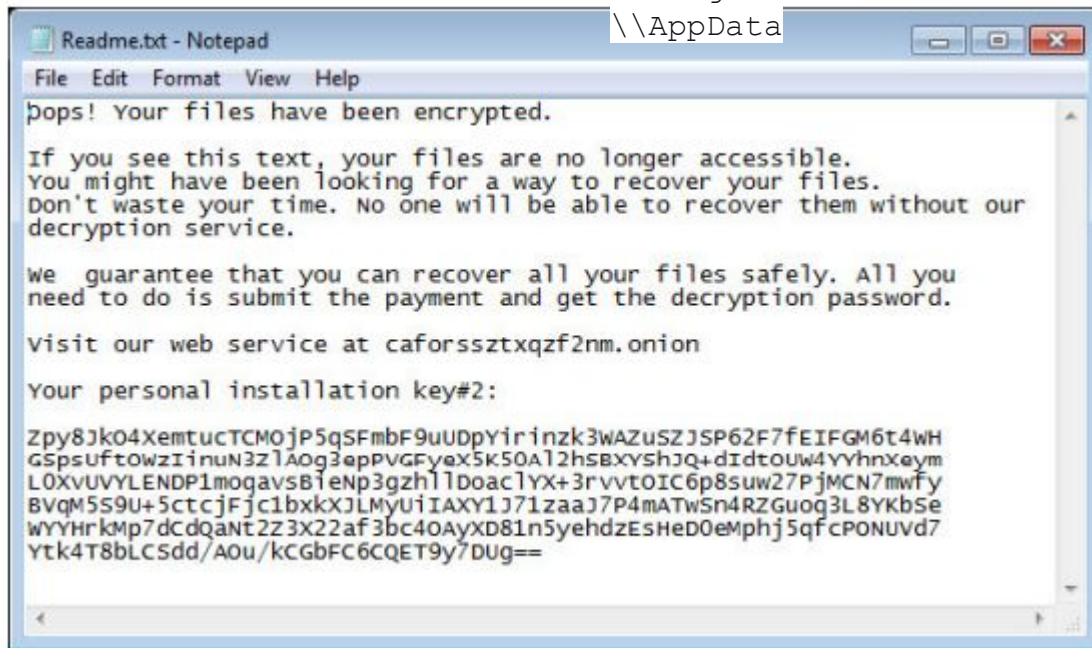
Some of the system directories are exempted from the attack:

File Encryption Process: **infpub.dat** also performs a major part of the encryption. **Readme.txt** is the list of the directories c:\Windows, c:\Program Files, c:\ProgramData, c:\AppData, etc, it

```
push    ebx                ; hTemplateFile
push    edi                ; dwFlagsAndAttributes
push    CREATE_NEW         ; dwCreationDisposition
push    edi                ; lpSecurityAttributes
push    edi                ; dwShareMode
push    40000000h          ; dwDesiredAccess
lea     eax, [ebp+FileName]
push    eax                ; lpFileName
call    ds:CreateFileW
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jz      loc_1000623C
```

```
lea     eax, [ebp+hLen]
push    eax                ; int
lea     eax, [esi+0Ch]
push    eax                ; Src
push    dword ptr [esi] ; int
mov     [ebp+hLen], edi
push    dword ptr [esi+30h] ; cbBinary
call    sub_100057E5
test    eax, eax
jz      short loc_10006235
```

```
push    1000h              ; Size
lea     eax, [ebp+Dst]
push    edi                ; Val
push    eax                ; Dst
call    memset
mov     esi, ds:StrCatW
add     esp, 0Ch
push    offset aDopsYourFilesH ; "Oops! Your Files have been encrypted.\r\n"
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
push    [ebp+hLen]
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
lea     eax, [ebp+Dst]
push    eax
call    esi ; StrCatW
lea     [ebp+NumberOfBytesWritten], edi
mov     ecx, [eax+2]
```



# How was the damage done?

## Lateral Movement:

1. GetExtendedTcpTable - which returns a list of active TCP connections.

2. GetIPNetTable - which gets the computer's ARP table, listing IP addresses and MAC addresses of computers in the same network segment

3. NetServerEnum - used to enumerate servers in the domain using a windows API function.

```
1000735B 56          push     esi
1000735C 57          push     edi
1000735D 68 10 16 01 10 push    offset aGetextendedtcp ; "GetEx
10007362 50          push     eax          ; hModule
10007363 FF 15 04 D2 00+call    ds:GetProcAddress
10007369 8B F8       mov     edi, eax
1000736B 85 FF       test    edi, edi
1000736D 0F 84 A1 00 00+jz     loc_10007414
```

```
1000753C 50          push     eax          ; bufptr
1000753D 6A 65       push     65h          ; level
1000753F 56          push     esi          ; servername
10007540 89 75 FC    mov     [ebp+Buffer], esi
10007543 89 75 F8    mov     [ebp+entriesread], esi
10007546 89 75 F0    mov     [ebp+totalentries], esi
10007549 89 75 F4    mov     [ebp+resume_handle], esi
1000754C FF 15 80 D2 00+call    ds:NetServerEnum
10007552 3B C6       cmp     eax, esi
10007554 74 0C       jz      short loc_10007562
```

```
10007430 33 FF       xor     edi, edi
1000743C 57          push     edi          ; Order
1000743D 8B 45 FC    lea     eax, [ebp+SizePointer]
10007440 50          push     eax          ; SizePointer
10007441 57          push     edi          ; IpNetTable
10007442 89 7D F0    mov     [ebp+var_10], edi
10007445 89 7D FC    mov     [ebp+SizePointer], edi
10007448 FF D6       call    esi ; GetIpNetTable
1000744B 3D E8 00 00 00 cmp     eax, 0E8h
1000744F 75 07       jnz     short loc_10007458
```



# How was the damage done?

## Lateral Movement:

Gaining local credentials using Mimikatz

Next,  
C:\Win  
name

```
100071A6 50          push    eax
100071A7 53          push    ebx
100071A8 53          push    ebx
100071A9 50          push    eax
100071AA FF 15 FC D0 00+call    ds:GetTempFile
100071B0 85 C0       test    eax, eax
100071B2 0F 84 60 01 00+jz     loc_10007318
```

```
10007272 8D 85 74 E9 FF+lea    eax, [ebp+CommandLine]
10007278 68 E0 15 01 10 push    offset aWsws ; "\\?ws\" %ws"
1000727D 50          push    eax ; LPWSTR
1000727E 89 7D 8C     mov     [ebp+Dst], edi
10007281 FF D6       call    esi ; wsprintfW
10007283 83 C4 1C     add     esp, 1Ch
10007286 8D 45 D0     lea     eax, [ebp+ProcessInformation]
10007289 50          push    eax ; lpProcessInformation
1000728A 8D 45 8C     lea     eax, [ebp+Dst]
1000728D 50          push    eax ; lpStartupInfo
1000728E 53          push    ebx ; lpCurrentDirectory
1000728F 53          push    ebx ; lpEnvironment
10007290 68 00 00 00 00 push    80000000h ; dwCreationFlags
10007295 53          push    ebx ; binheritHandles
10007296 53          push    ebx ; lpThreadAttributes
10007297 53          push    ebx ; lpProcessAttributes
10007298 8D 85 74 E9 FF+lea    eax, [ebp+CommandLine]
1000729E 50          push    eax ; lpCommandLine
1000729F 8D 85 74 F9 FF+lea    eax, [ebp+TempFileName]
100072A5 50          push    eax ; lpApplicationName
100072A6 FF 15 04 D1 00+call    ds:CreateProcessW
100072AC 85 C0       test    eax, eax
100072AE 74 23      jz      short loc_100072D3
```

the  
s to a

```
bytes]
urityAttributes
ultTimeOut
fferSize
ufferSize
nstances
eMode
nMode
e
```

Mimikatz is then executed from the temporary location with the named pipe as a parameter to obtain credentials stored in the local machine.

```
1000707D 56          push    esi ; lpOverlapped
1000707E 50          push    eax ; hNamedPipe
1000707F FF 15 08 D1 00+call    ds:ConnectNamedPipe
10007085 85 C0       test    eax, eax
10007087 0F 84 A2 00 00+jz     loc_1000712F
```



# How was the damage done?

## Lateral Movement:

Executing BadRabbit in new hosts

Sample usernames and passwords:

```
; "User"  
; "user"  
; "Admin"  
; "adminTest"  
; "test"  
; "root"  
; "123"  
; "1234"  
; "12345"  
; "123456"  
; "1234567"  
; "12345678"  
; "123456789"  
; "1234567890"
```

The malware now attempts to connect to the enumerated servers using obtained credentials. In addition, the malware contains a list of hardcoded usernames and passwords that are used as backup in order to authenticate (so it would not miss out on easily vulnerable targets).

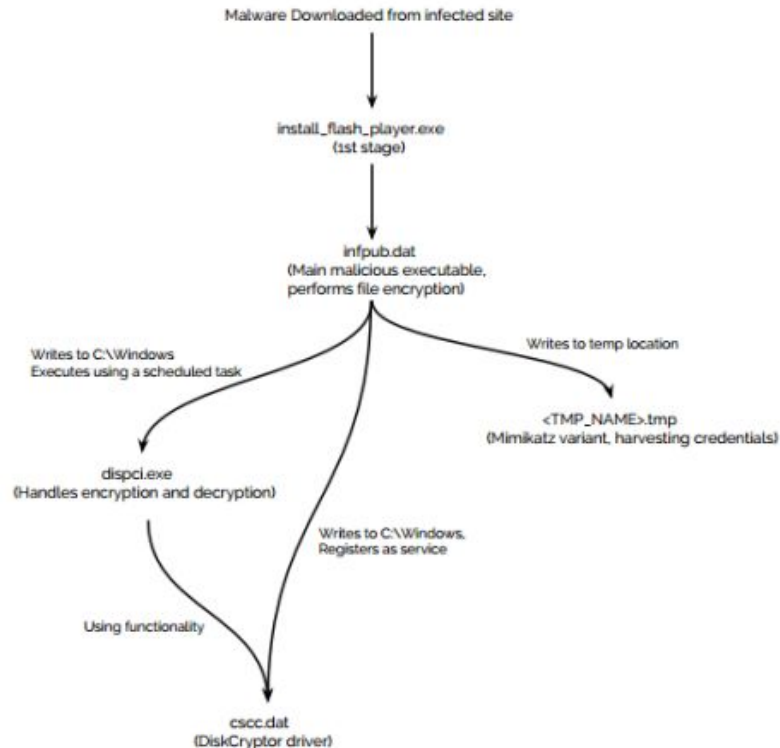
After the malware authenticates, it drops **"cscd.dat"** and **"infpub.dat"** in the "\\ admin\$" share:

```
10009582 8D 84 24 B0 02+lea    eax, [esp+0Ch+arg_29C]  
10009589 50                push   eax  
1000958A 53                push   ebx  
1000958B BF 98 19 01 10 nov    edi, offset aWAdminVs ; "\\ \\?us\\admin$\\?us"  
1000958C 8D 84 24 C0 0C+lea    eax, [esp+14h+FileName]  
1000958D 57                push   edi ; LPCWSTR  
1000958E 50                push   eax ; LPWSTR  
1000958F FF D6            call   esi ; wsprintfW  
10009590 33 C0            xor    eax, eax  
10009591 44 80 85 05 00+mov    eax, dword ptr [esp+14h+arg_29C]
```

And, the saga continues...

# Installation in a nutshell:

The following chart highlights the main functionality of the files used by the malware:



# What and Where were the targets?

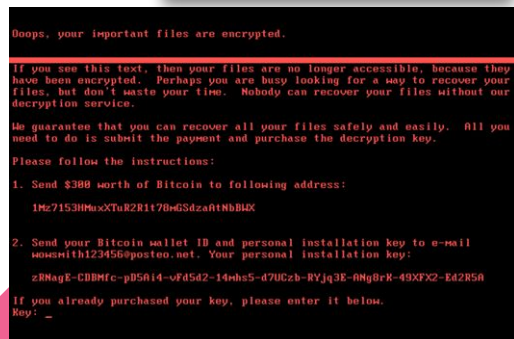
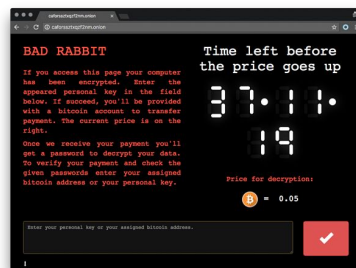
- May have been a targeted attack aimed at corporate networks.
- Targeted Eastern European countries.
- It infected government, media, transportation and corporate networks in 15 countries, including Russia's Interfax and Fontanka (news agencies), Ukraine's Kiev Metro, the Odessa International Airport, the Odessa naval port and various ministries of infrastructure and finance.



# Frankensteined Petya/NotPetya (aka EternalPetya) Clone ?



- Stolen petya kernel has been substituted with a more advanced DiskCryptor with a legitimate driver (stuxnet strategy?)
- Non destructive attack. The disk can be decrypted with a valid password.
- Does not use the EternalBlue and EternalRomance exploits.
- NotPetya was used a Ukraine-based company's update server, while Bad Rabbit uses drive-by downloads as an attack vector.
- Both NotPetya and Bad Rabbit use SMB to spread.
- Similar Ransom Screens.
- Bad Rabbit and NotPetya's DLL (dynamic link library) share 67 % of the same code.
- The two campaigns are "linked" to a cybercriminal group named **TeleBots**. (aka **Sandworm group** aka **BlackEnergy**) believed to be a subunit of APT28/PawnStorm/**Fancy Bear**/Sofacy/Tsar Team/Strontium/Sednit.
- **Associated with Russian military intelligence (GRU)**



# How to Mitigate Damage

- ★ Block the execution of files `c:\windows\infpub.dat` and `c:\Windows\scsc.dat` using Group Policy.
- ★ Disable WMI service (if it's possible in your environment) to prevent the malware from spreading over your network.

## Tips for everyone:

- Backup your data.
- Don't pay the ransom.
- Lock down admin accounts.  
Run as a standard user.
- **Educate Users.**
- **Don't just click. Double check.**



# Sources & Reports:

- <https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/>
- <https://securelist.com/bad-rabbit-ransomware/82851/>
- <https://threatpost.com/badrabbit-ransomware-attacks-hitting-russia-ukraine/128593/>
- <https://www.bleepingcomputer.com/news/security/bad-rabbit-ransomware-outbreak-hits-eastern-europe/>
- <https://unit42.paloaltonetworks.com/threat-brief-information-bad-rabbit-ransomware-attacks/>
- [https://threatvector.cylance.com/en\\_us/home/threat-spotlight-bad-rabbit-ransomware.html](https://threatvector.cylance.com/en_us/home/threat-spotlight-bad-rabbit-ransomware.html)
- [https://www.nyotron.com/collateral/Nyotron-BadRabbit-Report\\_FINAL.pdf](https://www.nyotron.com/collateral/Nyotron-BadRabbit-Report_FINAL.pdf)
- <https://sourceforge.net/projects/diskcryptor/>
- <https://www.offensive-security.com/metasploit-unleashed/mimikatz/>
- <https://arstechnica.com/information-technology/2017/06/notpetya-developers-obtained-nsa-exploits-weeks-before-their-public-leak/>
- <https://blog.skyboxsecurity.com/bad-rabbit-uses-social-engineering/>
- <https://www.darkreading.com/endpoint/bad-rabbit-dies-down-but-questions-remain/d/d-id/1330224>
- <https://www.tripwire.com/state-of-security/featured/october-2017-the-month-in-ransomware/>
- [https://www.theregister.co.uk/2017/10/26/bad\\_rabbit\\_post\\_mortem/](https://www.theregister.co.uk/2017/10/26/bad_rabbit_post_mortem/)
- <https://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/>
- <https://threatpost.com/bad-rabbit-linked-to-expetrnot-petya-attacks/128611/>
- <https://www.welivesecurity.com/2017/10/24/kyiv-metro-hit-new-variant-infamous-diskcoder-ransomware/>