

Forum: [Hack Forums](#)

Thread: [Obfuscated .Net app that drives me crazy - too expensive and it crashes](#)

TesterHack - August 13, 2025, 4:44 pm

I faced very big issues with Klennet ZFS Recovery. I have 2 destroyed ZFS drives. The app is the only one that recognizes real file structure and file state. Almost all of the files are OK. While they're not important I want to keep them. But the app is crashing on the drive 2. And it's \$400 (as I can use it only for drive 1 which is not a deal).

The developer does not respond and I'm unable to understand the logic. There is a function that calls .Invoke on some reflection. I see the commands, but when it goes inside a function, I don't see the code. It's EAZFuscator or similar.

2 things possible for free version - any ZFS volume with files is recognized and there is a Copy button. After the dialog it wants a registration. There is some check if registered (not able to understand the code). Also there is registration window. It calls a web service with some parameters and some other parameters are returned. All by reflections 1 by 1. I see the commands and the parameters, but I don't understand the logic (what should be returned) to make a hosts remap and a local WS.

For the crash and the way it works maybe I need it deobfuscated. Maybe it's hidden somewhere in the obfuscated classes' calls which do not split on reflection calls. It full of try-catch code, too.

```
[contract=tid]Start Contract[/contract]
```

Chornaya Magiya - August 13, 2025, 5:13 pm

Set up a local web proxy like Fiddler or Burp Suite. Intercept all outgoing web requests from Klennet's app. Monitor the registration request sent to the remote server, capturing all parameters.

Analyze the registration request and response. Save the exact request parameters the app sends and capture the server's response that validates the registration.

Modify your system's hosts file to redirect the app's registration server domain to 127.0.0.1 (your local machine). This makes the app send registration requests to your own computer instead of the real server.

Run a simple local HTTP server, such as Python's http.server or a basic NodeJS server. Serve the saved valid registration response when the app requests it. This fakes a successful registration reply from the server.

TesterHack - August 15, 2025, 2:12 am

I already did this, but it seems the response is not so simple.

```
"START\r\nZR\r\n2057\r\n{e3d03ac9-5f53-4c52-a36a-64b15f841b98}\r\n\r\n0\r\nC\r\nJHFJ-JHGJ-F  
GJF-JGHF-JGHJ\r\n4807\r\nTRATS"
```

```
POST-> [0] "http: //w1.klennet.com/e.aspx" object {string}
```

New String introduced: obj "START\r\n-1\r\n96\r\nTRATS" object {string} (count = 4)

In Fiddler I see that, too. The first string sent is somehow encoded and I suspect there is datetime functions used. (otherwise they're part of the telemetry timer)

The response is 4 rows: START -1 96 TRATS (which is START reversed). That results in no

licensing.

I'm unable to decode inside the functions to see the logic. For the moment I tried with HARMONY .Net and Extreme Injector, but with no success. I also created native DLL loader for the Harmony project - second DLL where I log. It's just not logging, but I don't try hard as it would log what's in .Invoke and it would log SOME of the logic only - with class.function calls, but not inside these functions. In some of them is the WS return decode logic.

If I find a way to deobfuscate and de-arm the app, maybe I'll find a way to fix this license problem + fix the crash issue on Disk2.

Till the moment only EAZFIX has solved some problems - vars are mostly visible, while the app is still working. If I try other cleanup or de4dot or something else on this app, the result is non-working app.

Here some notes: (by execution order). It's 30-60 minutes debugging, while the service request process repeated - as I changed some compare string returns.

ZfsRecovery-eazfix.exe

#=qtvVRxkVV..CMZ0= (class of the virtual execution)

row: 6705 - Send for Execution (breakpoint)

row: 4773 - obj - return, obj2 - object values (breakpoint)

"http: //logging.klennet.com/accept.aspx"

obj "http: //logging.klennet.com/accept.aspx" object {string}

@ "HKEY_CURRENT_USER\Software\Klennet\ZfsRecovery"

[0] "START" string

[1] "ZR" string

[2] "2057" string

[3] "{e3d03ac9-5f53-4c52-a36a-64b15f841b98}" string

[4] "" string

[5] "0" string

[6] "C" string

[7] "JHFJ-JHGJ-FGJF-JGHF-JGHJ" string (my test random key)

[8] "" string

[9] "TRATS" string

[0] {#=zCpAf0pV4JI7f_psh7Q==.#=zUsr2l84=} object {#=zCpAf0pV4JI7f_psh7Q==.#=zUsr2l84=}

[0] "START" string

[1] "ZR" string

[2] "2057" string

[3] "{e3d03ac9-5f53-4c52-a36a-64b15f841b98}" string

[4] "" string

[5] "0" string

[6] "C" string

[7] "JHFJ-JHGJ-FGJF-JGHF-JGHJ" string

[8] "4807" string

[9] "TRATS" string

"START\r\nZR\r\n2057\r\n{e3d03ac9-5f53-4c52-a36a-64b15f841b98}\r\n\r\n0\r\nC\r\nJHFJ-JHGJ-F
GJF-JGHF-JGHJ\r\n4807\r\nTRATS"

POST-> [0] "http: //w1.klennet.com/e.aspx" object {string}

New String introduced: obj "START\r\n-1\r\n96\r\nTRATS" object {string} (count = 4)

Again main link - return the same HTML

Assembly Check:

```
{Name = "#=zqZeWvpZqCiLbA2rfwAzOkmc=" FullName = "#=zqZeWvpZqCiLbA2rfwAzOkmc="}  
{#=zKy_9epaC73CZxpgW3g2t8hE= #=zOmE_MXrGZ$iJ())}
```

#=zXbzzYB0= - a class that defines the command

.Name = lme -> CompareString -> returns 1 when different

```
{Void SetProjectError(System.Exception)}
```

again logging at:

"http: //logging.klennet.com/accept.aspx" (i;w;l)

Probably the response check:

```
{Name = "#=z9sbZVqSBN$8GaOfHg==" FullName = "#=z9sbZVqSBN$8GaOfHg=="}  
{Int32 CompareString(System.String, System.String, Boolean)}
```

Reflection of a class

Service: "START\r\n-1\r\n96\r\nTRATS"

Note: I put space after all HTTP as I cannot post links despite it's debugging context.