

Forum:[Hack Forums](#)

Thread: [Does a BIN leave traces?](#)

Nickname. - August 20, 2016, 4:31 am

Okay so title says it pretty much,

What kind of traces does a BIN leave.

So the file you make with your builder. (Stub)

What kind of info can you find in the bin? That could trace to yourself

Rhez - August 20, 2016, 5:22 am

The stub contain your info like email/password/dns address/port/etc and it was encrypted(not all the time). When your stub was reverse engineered, then all your info will be exposed.

Talking on a RAT Stub, it will leave some traces on your clients like if you disable taskmanager/cmd, registry will be changed.

Purple Kief - August 20, 2016, 5:25 am

Everything you configure inside of your builder will be left behind by your bin.

Vuln - August 20, 2016, 5:29 am

It all depends on the RAT (and crypter if one is used) and its settings. The startup method would probably be the most common "trace" (apart from the process and the file itself obviously). It is usually either a registry key, a scheduled task, or an executable file in the Startup folder.

And keep in mind that some programs or (router) firewalls may be monitoring and logging outbound connections.

(Aug 20, 2016 04:31 AM)Unknown000 Wrote: [\[CITE\]](#) What kind of info can you find in the bin? That could trace to yourself

Everything your stub can do is stored (at least initially, but usually forever) in the stub itself. This includes your DNS hostname (IP address and port number), considering it has to connect to the server.

Nickname. - August 20, 2016, 5:46 am

(Aug 20, 2016 05:22 AM)Rhez Wrote: [\[CITE\]](#) The stub contain your info like email/password/dns address/port/etc and it was encrypted(not all the time). When your stub was reverse engineered, then all your info will be exposed.

Talking on a RAT Stub, it will leave some traces on your clients like if you disable taskmanager/cmd, registry will be changed.

How about my mac adress does that leave any traces?

(Aug 20, 2016 05:29 AM)Jailbyte Wrote: [\[CITE\]](#) It all depends on the RAT (and crypter if one is used) and its settings. The startup method would probably be the most common "trace" (apart from the process and the file itself obviously). It is usually either a registry key, a scheduled task, or an executable file in the Startup folder.

And keep in mind that some programs or (router) firewalls may be monitoring and logging outbound

connections.

Everything your stub can do is stored (at least initially, but usually forever) in the stub itself. This includes your DNS hostname (IP address and port number), considering it has to connect to the server.

So what would be the best way too work?

So if I would use a RDP for a rat then the binary can never trace back to my computer right.

Mr 4rs4l4ne - August 20, 2016, 6:07 am

When you finish your job, u need to uninstall your stub from your victim pc.

Have a good day .

Nickname. - August 20, 2016, 6:08 am

(Aug 20, 2016 06:07 AM)Mr 4rs4l4ne Wrote: [\[CITE\]](#) When you finish your job, u need to uninstall your stub from your victim pc.

Have a good day .

Lol this would still leave traces

Vuln - August 20, 2016, 7:51 am

(Aug 20, 2016 05:46 AM)Unknown000 Wrote: [\[CITE\]](#) How about my mac adress does that leave any traces?

There are no [MAC addresses](#) stored in the stub, if that's what you're asking.

(Aug 20, 2016 05:46 AM)Unknown000 Wrote: [\[CITE\]](#) So if I would use a RDP for a rat then the binary can never trace back to my computer right.

Even if you managed to anonymously obtain an RDP that doesn't log anything at all, then the ISP most likely will.

Being completely untraceable by anyone is harder than you think, especially if you're not using public networks and computers.

But needless to say, most RAT users aren't getting traced, just because they aren't worth tracing.

Joey Pirtz - August 20, 2016, 8:04 am

FYI the term you are looking for is 'whaling'. Use the search function and you'll find plenty of tuts on how it's done and what you can find.