

Forum:[Hack Forums](#)

Thread: [RATs and Linux \(What happened to Java RATs?\)](#)

Suggestive - December 30, 2018, 9:45 pm

Hi, I'm looking for a RAT that'll let me admin a Linux OS from Windows, I've heard that a Java RAT is suitable for this but there aren't any in this forum anymore, I remember them being more popular a few years ago. Is there any good RAT out there that'll let me control a Linux OS? Also, do I need special/specific settings when crypting the stub before sending it to the Linux machine?

Thank you,
Suggestive

CyberStrike - December 30, 2018, 10:08 pm

(Dec 30, 2018 10:45 PM)Suggestive Wrote: [\[CITE\]](#) Hi, I'm looking for a RAT that'll let me admin a Linux OS from Windows, I've heard that a Java RAT is suitable for this but there aren't any in this forum anymore, I remember them being more popular a few years ago. Is there any good RAT out there that'll let me control a Linux OS? Also, do I need special/specific settings when crypting the stub before sending it to the Linux machine?

Thank you,
Suggestive

Foreword on Java: You need execution, be it the user or a bash script or whatever.

Well Linux what kind of target are you shooting for? Servers? If that is the case exploitation is probably your best bet, then using a reverse shell.. of course some servers have a VNC yet no admin worth their salt doesn't operate in a shell. If you are thinking that end user's are your target then yes maybe a jar file may work but still execution is needed. I am unsure why you would want anything but a shell to work in, although if you are uncomfortable with a shell then you will probably face less options. Most Linux users also don't have AV if they do it's probably ClamAV if they are using Yara and rules are updated then well you may have some issues as that user knows a bit more in regards to malware. I never have "crypted" anything for Linux, why do you crypt? Well generally to evade AV scantime maybe a bit into runtime with varying levels of success, you should denote that during runtime payloads(stubs) can and are often dumped. In Linux it's not too hard literally memdump or checking out /proc/#### and dumping.

Most Linux users also do not just grab whatever ELF file and run it, like that is drummed in your head that you inspect scripts and src code before running off and compiling, in addition always using trusted sources is once again drummed into our heads. I've been into Linux or Unix in one form or another since 1999 and I am glad to see that these things which are drummed into our heads as Linux users is still very common to be stated to users.

Suggestive - December 30, 2018, 10:19 pm

(Dec 30, 2018 11:08 PM)SilentWatch Wrote: [\[CITE\]](#) Foreword on Java: You need execution, be it the user or a bash script or whatever.

Well Linux what kind of target are you shooting for? Servers? If that is the case exploitation is probably your best bet, then using a reverse shell.. of course some servers have a VNC yet no admin worth their salt doesn't operate in a shell. If you are thinking that end user's are your target then yes maybe a jar file may work but still execution is needed. I am unsure why you would want

anything but a shell to work in, although if you are uncomfortable with a shell then you will probably face less options. Most Linux users also don't have AV if they do it's probably ClamAV if they are using Yara and rules are updated then well you may have some issues as that user knows a bit more in regards to malware. I never have "crypted" anything for Linux, why do you crypt? Well generally to evade AV scantime maybe a bit into runtime with varying levels of success, you should denote that during runtime payloads(stubs) can and are often dumped. In Linux it's not too hard literally memdump or checking out /proc/#### and dumping.

Most Linux users also do not just grab whatever ELF file and run it, like that is drummed in your head that you inspect scripts and src code before running off and compiling, in addition always using trusted sources is once again drummed into our heads. I've been into Linux or Unix in one form or another since 1999 and I am glad to see that these things which are drummed into our heads as Linux users is still very common to be stated to users.

Thank you for the answer. I'm actually targeting a normal computer, used by a very average person. I'm just inquiring about the compatibility of RATs with Linux, as the only thing I know now is that Java RATs do work but they're not around as much for some reason, is there any alternative? If anyone can refer me to a good Java (or any compatible) RAT that would be great

CyberStrike - December 30, 2018, 10:57 pm

(Dec 30, 2018 11:19 PM)Suggestive Wrote: [\[CITE\]](#) Thank you for the answer. I'm actually targeting a normal computer, used by a very average person. I'm just inquiring about the compatibility of RATs with Linux, as the only thing I know now is that Java RATs do work but they're not around as much for some reason, is there any alternative? If anyone can refer me to a good Java (or any compatible) RAT that would be great

Shells, preferably reverse shells you can make them in ELF/Python/Perl/BASH. Once again if you are looking to deploy a VNC have a GUI you probably are going to be hampered and persistence options will be limited. I hope that you know about Linux enough that I am not writing anything foreign to you.