

Forum:[Hack Forums](#)

Thread: [AVG/AVAST Detection Issue. CSHARP](#)

CASP3R - December 28, 2018, 4:37 pm

Hello, So basically i am getting a detection, After some digging i found out what is getting detected. Its this peace of code below.

How do i get around this detection? I have tried renaming the value and that didn't do anything. I have also tried copying the file to the startup folder.... Same detection. Any help is appreciated.

```
Code using (RegistryKey key =  
Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true))  
{  
    key.SetValue("conhost", "\"" + tempPath + text + "\"");  
}
```

Best Regards, CASPER ? ?

Nick (Name) - December 28, 2018, 7:51 pm

You should try another form of startup, there's plenty of other methods out there but using the registry is probably not the best idea. If you're not code signing, AV's are going to flag any 32bit executable attempting to write in this extremely common startup location.

NYANxCAT - December 28, 2018, 9:01 pm

Try this

<https://www.andreafortuna.org/dfir/malware-persistence-techniques/>

CASP3R - December 29, 2018, 5:45 am

(Dec 28, 2018 08:51 PM)Nick (Name) Wrote: [\[CITE\]](#) You should try another form of startup, there's plenty of other methods out there but using the registry is probably not the best idea. If you're not code signing, AV's are going to flag any 32bit executable attempting to write in this extremely common startup location.

Dont u need a certificate to code sign? Im pretty sure some crypters have them but i dont wanna crypt my file.

(Dec 28, 2018 10:01 PM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Try this

<https://www.andreafortuna.org/dfir/malware-persistence-techniques/>

Thanks man! Ill check it out.

NYANxCAT - January 2, 2019, 1:42 am

n.p man, I'm glad it helped