

Forum:[Hack Forums](#)

Thread: [steganography, embed exe in pixels of an image](#)

donotask - June 29, 2018, 8:06 am

anybody here know about stegosploit? i discoverd it talking to a irl friend that uses this to spread. its the process of embedding an exe in pixeles of a jpeg or png image, it is used for spreading. victim opens image and exe is downloaded and executed.

also it can be a url where the victims visits and just opens the web page and gets infectes, cybersecurity blogs talk about embedding exe s in ads through stegosploit.

im interested in knowing more about this.

also my irl friend talked to me about rootkits, he spreads those with stegosploit, he says its almost impossible to remove because it goes "between the bios and the os". he says with a rootkit you have access to the whole computer. if its like this, why arent rootkist used to spread? could someone steal bots from sellers if he installs rootkits on every bot he buys? every time the stub gets detected/botkilled he would still have access to the pc with the rootkit? or am i missing somehting?

Condescend - June 29, 2018, 8:14 am

Visit a website and automatically download, run, and get infected? Yeah... I don't think so.

Unless you're running on an earlier version of Windows, getting applications to autorun without the user invoking it isn't possible, as far as I know. If this were possible, every single fake website with auto-downloads would take advantage of it.

Rootkits can be placed in multiple places of the OS. It depends on the technique of the creator. They can be detected, but it can be pretty weird detecting them. They are also much more difficult to create, due to them being so much more advanced than other malware; and, most of the time, they take advantage of system vulnerabilities to gain more administrative access, so that makes them even harder to construct.

donotask - June 29, 2018, 10:03 am

(Jun 29, 2018 08:14 AM)Condescend Wrote: [\[CITE\]](#) Visit a website and automatically download, run, and get infected? Yeah... I don't think so.

Unless you're running on an earlier version of Windows, getting applications to autorun without the user invoking it isn't possible, as far as I know. If this were possible, every single fake website with auto-downloads would take advantage of it.

Rootkits can be placed in multiple places of the OS. It depends on the technique of the creator. They can be detected, but it can be pretty weird detecting them. They are also much more difficult to create, due to them being so much more advanced than other malware; and, most of the time, they take advantage of system vulnerabilities to gain more administrative access, so that makes them even harder to construct.

but could a rootkit download and execute a exe on a pc?

also check here about stegosploit and malvertising: [http s : / / theha ckernews.com/ 2016/12/ima ge- exp loit-hac king .htm l](http://thehackernews.com/2016/12/image-exploit-hacking.html) is this possible?

Condescend - June 29, 2018, 10:08 am

(Jun 29, 2018 10:03 AM)donotask Wrote: [\[CITE\]](#) but could a rootkit download and execute a exe on a pc?

also check here about stegosploit and malvertising: <https://thehackernews.com/2016/12/image-exploit-hacking.html> is this possible?

A rootkit usually has full administrative privileges, so yes; it could run an application at its will. I've never heard of malvertising.

Boolean type - June 29, 2018, 10:10 am

OP you are missing common sense also your friend is an idiot or retarded skid. Sorry i had to say that.

honestly never seen more bullshit in one thread.

donotask - June 29, 2018, 10:31 am

(Jun 29, 2018 10:10 AM)Boolean type Wrote: [\[CITE\]](#) OP you are missing common sense also your friend is an idiot or retarded skid. Sorry i had to say that.

honestly never seen more bullshit in one thread.
ok, but why?

Clarence - June 29, 2018, 11:17 am

(Jun 29, 2018 08:14 AM)Condend Wrote: [\[CITE\]](#) Visit a website and automatically download, run, and get infected? Yeah... I don't think so.

Isn't that like the way an exploit kit works though? I may be wrong

Justanotheralias - June 29, 2018, 12:02 pm

(Jun 29, 2018 10:10 AM)Boolean type Wrote: [\[CITE\]](#) OP you are missing common sense also your friend is an idiot or retarded skid. Sorry i had to say that.

honestly never seen more bullshit in one thread.
Thank you, I saved 2 minutes typing that.

Condend - June 29, 2018, 2:57 pm

(Jun 29, 2018 11:17 AM)Clarence Wrote: [\[CITE\]](#) Isn't that like the way an exploit kit works though? I may be wrong

Exploit kits take advantage of vulnerabilities in browsers, and the system and its applications in of itself. Years ago, autorunning downloaded executables was much more common, due to these kits, but due to them being so difficult to create, and the frequency of patches of software, they are not nearly as common.

That's why I said "unless you are running on an earlier version of Windows," because less updated machines are more vulnerable to exploits.

inyourmemory - June 29, 2018, 3:45 pm

(Jun 29, 2018 02:57 PM)Condend Wrote: [\[CITE\]](#) Exploit kits take advantage of vulnerabilities in browsers, and the system and its applications in of itself. Years ago, autorunning downloaded executables was much more common, due to these kits, but due to them being so difficult to create, and the frequency of patches of software, they are not nearly as common.

That's why I said "unless you are running on an earlier version of Windows," because less updated machines are more vulnerable to exploits.

EKs are the main infection vector (not the RIG shits)