

Forum:[Hack Forums](#)

Thread: [Botkill](#)

ProtectNull™ - April 10, 2014, 12:03 am

Can someone show me a simple or working source i want to have a understanding on how it works.

Thanks alot.

Madara-Uchiha - April 10, 2014, 12:14 am

There are differnent methods ofc.

One is to loop through all processes running, and compare byte pattern, so you can identify malware by a specific bytearray/string.

The other way would to use heuristic detection methods.

Check if the file is saved in suspicious locations like AppData, it uses reflection and maybe also has a startupkey. Then you can tell with a pretty good chance that this is a keylogger/trojan whatever.

ProtectNull™ - April 10, 2014, 1:24 am

(Apr 10, 2014 12:14 AM)Madara-Uchiha Wrote: [\[CITE\]](#) There are differnent methods ofc.

One is to loop through all processes running, and compare byte pattern, so you can identify malware by a specific bytearray/string.

The other way would to use heuristic detection methods.

Check if the file is saved in suspicious locations like AppData, it uses reflection and maybe also has a startupkey. Then you can tell with a pretty good chance that this is a keylogger/trojan whatever.

Thats a good explanation. +1. Do you have any codes that can show me this? PM me if you don't want to show it publicly.

FFace - April 10, 2014, 3:57 am

Most people loop trough the process list and check if it matches one in the blacklist. Or they check process' modules to see anything sketchy.

ProtectNull™ - April 10, 2014, 4:02 am

(Apr 10, 2014 03:57 AM)FFace Wrote: [\[CITE\]](#) Most people loop trough the process list and check if it matches one in the blacklist. Or they check process' modules to see anything sketchy.

Do you have a code to show on how this works?

FFace - April 10, 2014, 4:20 am

(Apr 10, 2014 04:02 AM)Matthewbmx™ Wrote: [\[CITE\]](#) Do you have a code to show on how this works?

I'm not in love with spoonfeeding but anyway:

This is how you kill it if it has a blacklisted process name
Code For each proc as process in process.getprocesses
If proc.processname = "blacklisted" then proc.kill
next

This is how you kill it if it has a blacklisted modulename

Code For each proc as process in process.getprocesses
For i as integer = 0 to proc.modules.count - 1
If modules(i).ModuleName = "blacklisted" then proc.kill

next

The code was not written in a IDE so there might be errors.

ProtectNull™ - April 10, 2014, 4:33 am

(Apr 10, 2014 04:20 AM)FFace Wrote: [\[CITE\]](#) I'm not in love with spoonfeeding but anyway:

This is how you kill it if it has a blacklisted process name

Code For each proc as process in process.getprocesses

If proc.processname = "blacklisted" then proc.kill

next

This is how you kill it if it has a blacklisted modulename

Code For each proc as process in process.getprocesses

For i as integer = 0 to proc.modules.count - 1

If modules(i).ModuleName = "blacklisted" then proc.kill

next

The code was not written in a IDE so there might be errors.

So technically it finds a selected process name and kills it? what happens if they place a random virus name like gaegaegageieano.exe?

FFace - April 10, 2014, 4:43 am

(Apr 10, 2014 04:33 AM)Matthewbmx™ Wrote: [\[CITE\]](#) So technically it finds a selected process name and kills it? what happens if they place a random virus name like gaegaegageieano.exe?
I think I said it's just a basic one.