

Forum: [Hack Forums](#)

Thread: [\[Development\] Apollo IRC Bot.](#)

Break - January 22, 2013, 5:58 pm

Information:

Apollo is a Windows IRC bot Written in C++. It uses IRC with the option of SSL to communicate with the C&C (command-and-control server). As a self-defense, Apollo also has rootkit to hide its presence on the created files and registry entries by intercepting Win32 API calls. Apollo performs a system wide hook to inject itself into the whole process. It installs to the users computer with a randomly generated filename and runs the file at startup.

Features:

User-Mode Rootkit

- Hooks NtQueryDirectoryFile, NtEnumerateValueKey, and others to keep Apollo's file and registry entries hidden from users and other malware.

Ruskill

- Downloads and runs file of the masters choice and removes it when rebooted.

Proactive Defense

- Monitors APIs to stop the installtion of other malware on the system.

DNS Redirector

- Blocks AV update sites and other domains of your choice.

DDoS

- Slowloris (Apache flood), UDP Flood (Rapidly sends UDP packets to specific IP), and SYN Flood (Rapidly sends SYN requests to specific IP) good for web servers.

Form Grabber

- Monitors POST requestes from web browsers capturing emails and passwords.

FTP Grabber

- Captures FTP details inputed by the user.

USB Spread

- Infects USB drives using .lnk and autorun.

Skype Spread

- Sends messages to infected users skype contacts. MSN is being ported to skype for those who didn't know.

MSN Spread

- Sends Messages to infected users msn contacts without the infected user knowing. Msn Will still be working in China after the msn to skype mitigation.

HTTP Spread

-Replaces status updates, chat messages, and private messages on Twitter and Facebook.

Project Status

Spoiler ([Click to View](#))

[?] = finished

[?] = Not done

[?] = next update

[?] User-Mode Rootkit

[?] Proactive Defense

[?] Registry Persistence

[?] DDoS

[?] Form grabber

[?] Ftp Grabber

[?] Usb Spread

[?] Msn Spread

[?] Http Spread

[?] Download/Update (Someone will ask if it is included or not)

[?] Skype spread

[?] Dns Blocker/Redirector

[?] Ruskil

[?] SSL Support for IRC Connection

[?] Sock4 server (with UPNP support.)

[?] Putty SSH Client login stealer.

[?] AntiVirus Disabler (Will be able to Disable over 25 Antivirus/firewall solutions)

Apollo IRC Bot is about 75% done at the moment I will be updating the thread as I work on this.
If you would like to be a beta tester Pm [AppData](#) a reason why and your knowledge with IRC Bots.
Thank you

lulz4days - January 22, 2013, 6:20 pm

Vouch, seen source code via TeamViewer.

Kernel Mode - January 22, 2013, 7:51 pm

Seen the source, Isn't copy and paste.

Light Yagami. - January 22, 2013, 7:52 pm

Well this looks good i vouch to and i can't wait until this well be released.

betamonkey - January 22, 2013, 8:04 pm

Also seen the source. Looks okay to me, not from anything I have seen.

Beta Monkey

zShotS is Back - January 22, 2013, 8:07 pm

You've always stood out among the skids lol.

I'm interested, very. What are the differences between the base and 4 modules?

AppData - January 22, 2013, 8:12 pm

@zShots is Back

The base is just the bot itself with the rootkit and main features. The 4 module package is your choose of Pdef, msn spread, http spread, Ftp grabber, Formgrabber, DDoS Modules.

zShotS is Back - January 22, 2013, 8:17 pm

(Jan 22, 2013 09:12 PM)AppData Wrote: [\[CITE\]](#) @zShots is Back

The base is just the bot itself with the rootkit and main features. The 4 module package is your choose of Pdef, msn spread, http spread, Ftp grabber, Formgrabber, DDoS Modules.

Okay if modules are just features, I'm assuming the full package is everthing. And I'd hope you'd be able to choose which modules you want.

AppData - January 22, 2013, 8:19 pm

(Jan 22, 2013 09:17 PM)zShotS is Back Wrote: [\[CITE\]](#) Okay if modules are just features, I'm assuming the full package is everthing. And I'd hope you'd be able to choose which modules you want. The full Package includes everything in the bot, and yes you do choose which modules you want to have.

hottrod - January 22, 2013, 9:48 pm

This bot looks really good, cant wait for it to get released.

?Mystical - January 23, 2013, 12:19 am

Seen the source not like anything i have seen, Should turn out to be a good irc bot.

AppData - January 23, 2013, 6:12 am

Ty for the people who posted about my source, if you have any questions feel free to pm me.

Thank you.

?

van1lle - January 23, 2013, 9:25 am

Good job mayne. Haven't seen any bot here which makes use of encrypted traffic.

mrkid0s - January 23, 2013, 10:16 am

I'm interested in the bot, but I need you to show me by teamviewer.
give me your contact.

Break - January 23, 2013, 11:27 am

I will update the thread later with screenshots of the code.

Linux-0 - January 24, 2013, 5:13 pm

seen the source, absolute garbage. C+P reptile.

AppData - January 24, 2013, 6:59 pm

@Linux-0

Sir you have not seen my source kindly leave the thread, The people who have seen my source have already commented on the thread. You have no idea what you are talking about. Good day.

?

keriboh - January 24, 2013, 7:35 pm

Seems like a good bot. might Pm you about it in the furture

Hacker16 - January 24, 2013, 8:01 pm

have to say. this will be an amazing bot. no c&p bullshit. coded from scratch. glws. i will be getting this once finished. ps.... src is nice.

MrPip - January 25, 2013, 7:48 am

Looks great, can't wait for it to be out !

AppData - January 25, 2013, 12:49 pm

Thank you for the vouches, I will be posting soon what is done so far on Apollo IRC bot.

cr0ss - January 26, 2013, 10:51 am

Looks nice and seems legit seeing that betamonkey posted on the thread.

whattheheck - January 26, 2013, 4:02 pm

(Jan 26, 2013 11:51 AM)cr0ss Wrote: [\[CITE\]](#) Looks nice and seems legit seeing that betamonkey posted on the thread.He posts the same shit in every bot development thread.

?

Linux-0 - January 28, 2013, 10:51 am

(Jan 24, 2013 07:59 PM)AppData Wrote: [\[CITE\]](#) @Linux-0

Sir you have not seen my source kindly leave the thread, The people who have seen my source have already commented on the thread. You have no idea what you are talking about. Good day.

?

Kid this bot is trash, i have seen the source. garbage.

wolf_mc12 - January 28, 2013, 2:11 pm

Apollo IRC bot > this bots is FAKE.

Break - January 28, 2013, 9:32 pm

(Jan 28, 2013 03:11 PM)wolf_mc12 Wrote: [\[CITE\]](#) Apollo IRC bot > this bots is FAKE.Can you explain to us how this bot is fake? lol get lost

?rthur - January 29, 2013, 8:52 am

In which language is it coded?

If you read this it means my message was not long enough :)

AppData - January 29, 2013, 8:39 pm

(Jan 29, 2013 09:52 AM)Arthur1472 Wrote: [\[CITE\]](#) In which language is it coded?
If you read this it means my message was not long enough :)Apollo IRC Bot is coded in C++
If you have any questions feel free to pm me.

?

___Digital___ - January 30, 2013, 2:20 pm

vouch for this and a good friend of mine told me about this bot looks awesome.. good luck with it

Cloud9™ - January 31, 2013, 12:10 pm

Amazing IRC bot is clearly amazing.

AppData - January 31, 2013, 2:21 pm

Thank you for the Comments & Vouches.

I am starting the SSL Support for IRC Connection today, Will update thread once done and fully working.

?

Oplichter - February 1, 2013, 6:37 am

Looks very good, also the feedback thats given on it hehe.

Good luck with this dude and i hope i can use it anytime ! :)

mrGRINCH - February 1, 2013, 10:17 am

Just had a look and the source for this and it looks quite interesting.

zezaku - February 2, 2013, 5:35 am

Waiting for rocky balboa bot soon now that apollo is here

Good-Luck - February 2, 2013, 6:25 am

Good luck for the project :D !! ((35))

Disfigure - February 2, 2013, 8:22 am

bot looks really nice im sure a lot of people will like it

StephenRoos - February 2, 2013, 11:39 am

(Jan 22, 2013 06:58 PM)Break Wrote: [\[CITE\]](#) User-Mode Rootkit

-Hooks NtQueryDirectoryFile, NtEnumerateValueKey, and others to keep Apollo's file and registry entries hidden from users and other malware.

x86 and x64?

I'd also be curious to verify the source for this.

AppData - February 2, 2013, 11:50 am

(Feb 2, 2013 12:39 PM)StephenRoos Wrote: [\[CITE\]](#) x86 and x64?

I'd also be curious to verify the source for this.Only works on x86 next version will be working on x64, Also many people have seen and vouched for my source so there is no need for you to have a look at it.

?

StephenRoos - February 2, 2013, 12:24 pm

(Feb 2, 2013 12:50 PM)AppData Wrote: [\[CITE\]](#) Only works on x86 next version will be working on x64, Also many people have seen and vouched for my source so there is no need for you to have a look at it.

?

I would think the more the merrier, but fair enough.

In that case, may I ask what method of hooking you are using? Is it a standard inline splice in the prologue of all targeted APIs, or something more advanced?

NexxioN2 - February 2, 2013, 3:22 pm

This bot seems to be nice, I cant wait untill its released.

StephenRoos - February 3, 2013, 1:46 pm

AppData recently allowed me to look at the source code.

Based on what I saw, I will say with confidence that:

-It is not a rip of any public source that I have ever seen (and I've seen a lot).

-The programmer has at least a basic understanding of malware design, the Windows API, the C++ programming language, and code organization. In short, he has the skill set required to author the bot described in the original post.

It is important to bear in mind that what betamonkey said is essentially true: No matter who the person in question might be, no one can ascertain that it is either a "good" or "bad" product just from flipping through the source for two minutes. I am not an exception. Saying anything more than what I've said would be guessing at best. I suggest that both the shit-slinging and ecstatic vouching be saved for when the product is actually available.

canttouchthis - February 4, 2013, 3:03 am

ssl using openssl libraries?

disis

AppData - February 4, 2013, 6:11 am

(Feb 4, 2013 04:03 AM)canttouchthis Wrote: [\[CITE\]](#) ssl using openssl libraries?

disisNo sir, That would make the bot very bloated.

?

inet_addr - February 5, 2013, 9:05 am

Looks like a great bot, good luck with sales!

Break - February 6, 2013, 5:40 am

Thanks for all the positive comments guys. If you have any concerns or questions about Apollo pm AppData.

Knegarachi - February 6, 2013, 7:32 am

Lol damn. How do I get one of these?

kodakiller - February 6, 2013, 12:21 pm

this looks good, ill be looking for a release :)

AppData - February 8, 2013, 8:03 pm

Update 2/8: Dns Blocker/Redirector is finished and fully working. If you have any questions about Apollo IRC Bot feel free to pm me.

?

Antagonism - February 8, 2013, 8:09 pm

Does it have an add to startup option ?

If yes, how do you add the file to system registry ?

Just saying because most methods are detected, as well as userland hooks..

dcyber1 - February 8, 2013, 8:23 pm

Looks pretty good. :)

How can I get this one?

betamonkey - February 8, 2013, 8:28 pm

(Feb 8, 2013 09:09 PM)Antagonism Wrote: [\[CITE\]](#) Does it have an add to startup option ?

If yes, how do you add the file to system registry ?

Just saying because most methods are detected, as well as userland hooks..

'Detected' is such a generic term. Most AVs look at the sum of the actions performed up to a certain point, and not just start bitching on one singular event.

Antagonism - February 8, 2013, 9:05 pm

(Feb 8, 2013 09:28 PM)betamonkey Wrote: [\[CITE\]](#) 'Detected' is such a generic term. Most AVs look at the sum of the actions performed up to a certain point, and not just start bitching on one singular event.

That's true, but you need to be sure to make proper tests to be sure it is not detected by AVs. If you coded it from scratch, you should not have problems with that.

betamonkey - February 8, 2013, 9:13 pm

(Feb 8, 2013 10:05 PM)Antagonism Wrote: [\[CITE\]](#) That's true, but you need to be sure to make proper tests to be sure it is not detected by AVs. If you coded it from scratch, you should not have problems with that.

Right, well, it's up to the authors here to do the proper tests. I can guarantee there will be issues though for some of the stuff. Usually is unless they were incredibly innovative from the get-go.

Antagonism - February 8, 2013, 9:50 pm

(Feb 8, 2013 10:13 PM)betamonkey Wrote: [\[CITE\]](#) Right, well, it's up to the authors here to do the proper tests. I can guarantee there will be issues though for some of the stuff. Usually is unless they were incredibly innovative from the get-go.

That's why the beta version will be a must if they want a successful product.

While we are at it, I'm not well experienced with blackhats programs, as I only code legitimate programs. But I see the bot is using usermode rootkit. Would not it be better to use kernel mode (Ring0) ? As it's the most privileged ring ?

betamonkey - February 8, 2013, 9:53 pm

(Feb 8, 2013 10:50 PM)Antagonism Wrote: [\[CITE\]](#) That's why the beta version will be a must if they want a successful product.

While we are at it, I'm not well experienced with blackhats programs, as I only code legitimate programs. But I see the bot is using usermode rootkit. Would not it be better to use kernel mode (Ring0) ? As it's the most privileged ring ?

Yes that is always ideal if the coder can do it, and if they can properly load a KMD. Actually installing a driver or inserting code into ring0 is the hard part. There are limited ways and they only get more and more complicated the slicker you get.

Plus if you do it in such a way that requires dropping to disk (most ways), then you have to deal with encrypting a driver file each time. When it comes to malware there usually is always a better way but whether it is practical in most situations is rarely the case.

Beta Monkey

Antagonism - February 8, 2013, 10:15 pm

(Feb 8, 2013 10:53 PM)betamonkey Wrote: [\[CITE\]](#) Yes that is always ideal if the coder can do it, and if they can properly load a KMD. Actually installing a driver or inserting code into ring0 is the hard part. There are limited ways and they only get more and more complicated the slicker you get.

Plus if you do it in such a way that requires dropping to disk (most ways), then you have to deal with encrypting a driver file each time. When it comes to malware there usually is always a better way but whether it is practical in most situations is rarely the case.

Beta Monkey

Ah, I see. Funniest thing is that a rootkit is not necessarily a malware. But obviously, this technology has been used for malwares, as the goal is to "hide" itself from the user and obviously, AVs.

A kernel mode rootkit could be almost impossible to remove and could require a reinstallation of the operating system, so it's obvious it's the best option.

Also, I always thought rootkits needed admin rights or root to be executed. I suppose it has not taken much time that someone found out how to bypass the verification using a known vulnerability..

Thanks for your constructive replies BetaMonkey, this is much appreciated ?

betamonkey - February 8, 2013, 10:18 pm

(Feb 8, 2013 11:15 PM)Antagonism Wrote: [\[CITE\]](#) Ah, I see. Funniest thing is that a rootkit is not necessarily a malware. But obviously, this technology has been used for malwares, as the goal is to "hide" itself from the user and obviously, AVs.

A kernel mode rootkit could be almost impossible to remove and could require a reinstallation of the operating system, so it's obvious it's the best option.

Also, I always thought rootkits needed admin rights or root to be executed. I suppose it has not taken much time that someone found out how to bypass the verification using a known vulnerability..

Thanks for your constructive replies BetaMonkey, this is much appreciated ?

Privilege escalation exploits are usually patched quickly. Windows Update service checks daily so nowadays they are only good as long as they are unpatched. Obviously working at the same level as the OS is ideal but getting to that point is difficult when you factor in AntiViruses, requiring elevation and then the difficulty of writing a stable, effective rootkit in the first place. It's really the

kind of thing you have to invest a good deal of effort into, and not worth it if you do it half-assed.

Beta Monkey

kayone - February 11, 2013, 5:21 pm

(Feb 8, 2013 09:03 PM)AppData Wrote: [\[CITE\]](#) Update 2/8: Dns Blocker/Redirector is finished and fully working. If you have any questions about Apollo IRC Bot feel free to pm me.

?

Please get back to my PM, thank you dude!

Kernel Mode - February 12, 2013, 1:22 am

(Feb 8, 2013 11:15 PM)Antagonism Wrote: [\[CITE\]](#) Ah, I see. Funniest thing is that a rootkit is not necessarily a malware. But obviously, this technology has been used for malwares, as the goal is to "hide" itself from the user and obviously, AVs.

A kernel mode rootkit could be almost impossible to remove and could require a reinstallation of the operating system, so it's obvious it's the best option.

Also, I always thought rootkits needed admin rights or root to be executed. I suppose it has not taken much time that someone found out how to bypass the verification using a known vulnerability..

Thanks for your constructive replies BetaMonkey, this is much appreciated ?

Actually most kernel mode rootkits aren't any harder than a good ring 3 rootkit, to remove.

Prank Calling - February 15, 2013, 8:51 pm

bot looks good cant wait for release.

cr0ss - February 20, 2013, 9:19 pm

(Feb 12, 2013 02:22 AM)Kernel Mode Wrote: [\[CITE\]](#) Actually most kernel mode rootkits aren't any harder than a good ring 3 rootkit, to remove.

Yeah, you just simply open cd-rom , place dick , and shuit it.

DISC1 - February 20, 2013, 11:22 pm

Keep me posted on this issue because i need some good bots