

Forum:[Hack Forums](#)

Thread: [The "LOL" Facebook message infection \[.jar dropper | CPU Miner | Keylogger\]](#)

Aura - May 20, 2014, 11:20 am

Hey guys, Aura here with yet another warning.

Recently, a new malware came up on Facebook. This malware is sent in a Facebook message that contains "lol" and a link to a .zip attachment that is named "IMG_xxxx.zip". The message can also contains "OMG" or "Have a look at this", even "I can't believe someone posted this" (back in the days of MSN). Inside the .zip is a file named "IMG_xxxx.jar". For those who do not have the "Hide file extensions for known extension type" on Windows, they won't notice that the file is actually a .jar (executable Java file) and not a .png, .jpg or any other popular picture format. This .jar isn't the main malware but a downloaders/dropper that downloads the malware from a Dropbox shared folder and then installs it on the victim's computer. This malware install itself as a service, therefore it is very persistant. Also, this malware will then spread throught the victim's Facebook friend list using the same kind of message the victim got infected by in the first place. Therefore this file is asumed to be a worm but also a CPU Miner from what the last report from users in the White Hat Help section says. This malware have been identified as a variant of the Zusy Trojan that usually hooks itself into web browsers in order to steal personal information, mostly credit card numbers and other financial data.

If you come across one of these message and file, please warn the person that sent it to you that he'S infected and should get his system checked up immediately.

I'm posting this as I recently assisted a user with this issue in the White Hat Help section. The malware isn't hard to remove for experienced malwares removal members like myself, Maitricks, Arr, Null Byte, etc. but can be a bit tricky for people who never faced this kind of malware.

Once again please keep in mind to always use an Antivirus at all time and also to now download anything fishy from the web and ALWAYS verify your downloads in Sandboxie or a VM before using them on your host system.

Original article on TheHackersNews : [LOL, Jar File Malware Just Goes Viral Through Facebook Messages](#)

Thank you and stay safe everyone.

ShadowWolf - May 20, 2014, 12:45 pm

Good to know, will be more careful on facebook now. Not that I am not careful anyway.

R?DSPY - May 20, 2014, 12:45 pm

Sometimes I download those on purpose to see what it will do.
I run it in sandboxie.

Aura - May 20, 2014, 12:56 pm

(May 20, 2014 12:50 PM)legend7 Wrote: [\[CITE\]](#) Make sure you have Sandboxie set to deny Internet access. It could be stealing login information.

I don't have this settings on my Sandboxie as I run it in a VM where no passwords or login have ever been stored so it allows me to push the tests a bit more far.

Jagster™ - May 20, 2014, 1:03 pm

Tell me how to check for it and how to remove (not for me but for others :P), that way you won't have 1k check-up requests :)

Aura - May 20, 2014, 1:04 pm

(May 20, 2014 01:03 PM)Jagster™ Wrote: [\[CITE\]](#) Tell me how to check for it and how to remove (not for me but for others :P), that way you won't have 1k check-up requests :)

Shit, I should really start to create documentation on every new malwares I remove and then send it to you guys ?

Aura - May 20, 2014, 1:06 pm

(May 20, 2014 01:05 PM)legend7 Wrote: [\[CITE\]](#) I do the same. Although I think my Windows 7 VM just expired. ?

Also, I remember a few years ago when there was a worm spreading through Skype that did essentially the same thing as this. It sent messages that said "hey is this your new profile pic <insert link to .exe disguised as a picture here>".

You don't have to activate a Windows VM lol. Mine are all expired and I don't care.

Aura - May 20, 2014, 1:13 pm

(May 20, 2014 01:10 PM)legend7 Wrote: [\[CITE\]](#) I think they went from requiring activation to just trying to annoy you into activating but not actually making it mandatory. ?

Yeah you just click "Skip" and "Activate later" and it leaves you alone so it's not that bad.

Dr. Manhattan - May 20, 2014, 1:14 pm

Yeah i've got friends that were also infected by this kind of malware. I really can't help them in removing it, i just warn them about what they are facing now : (

Aura - May 20, 2014, 1:37 pm

(May 20, 2014 01:14 PM)Dr. Manhattan Wrote: [\[CITE\]](#) Yeah i've got friends that were also infected by this kind of malware. I really can't help them in removing it, i just warn them about what they are facing now : (

Tell them to sign up on HackForums and head straight up for the MRT section ?

ShadowWolf - May 20, 2014, 1:52 pm

(May 20, 2014 01:04 PM)Aur? Wrote: [\[CITE\]](#) Shit, I should really start to create documentation on every new malwares I remove and then send it to you guys ?

Perhaps someone should create a thread where people post new malware they find and how they have solved it. That way people trying to expand their knowledge could go and learn new methods or how to to identify certain malwares.

Aura - May 20, 2014, 1:55 pm

(May 20, 2014 01:52 PM)ShadowWolf Wrote: [\[CITE\]](#) Perhaps someone should create a thread where people post new malware they find and how they have solved it. That way people trying to expand their knowledge could go and learn new methods or how to to identify certain malwares.

The thing with this thread is that only allowed and recognized helper like me should be trusted. We would have to manually verify all the other methods posted.

Motix - May 20, 2014, 1:58 pm

Thanks for notifying, I'll be more careful and I'll also notify people I know about this so they won't fall

for this. Thanks again! :)

grady - May 20, 2014, 2:10 pm

There is actually the same type of thing but for Skype.
I had a friend infected by it.

Aura - May 20, 2014, 2:11 pm

(May 20, 2014 01:58 PM)iOhh Wrote: [\[CITE\]](#) Thanks for notifying, I'll be more careful and I'll also notify people I know about this so they won't fall for this. Thanks again! :)
No problem buddy, stay safe.

(May 20, 2014 02:10 PM)?Infamy Wrote: [\[CITE\]](#) There is actually the same type of thing but for Skype.

I had a friend infected by it.

I guess the worm has been modified to it spreads through other means. Facebook and now Skype as well.

grady - May 20, 2014, 2:13 pm

(May 20, 2014 02:11 PM)Aur? Wrote: [\[CITE\]](#) No problem buddy, stay safe.

I guess the worm has been modified to it spreads through other means. Facebook and now Skype as well.

It's been on Skype for quite some time actually, I'm pretty sure it was originally for Skype and this Facebook version is a new strain of it.

The Skype message was the same type of thing that you mentioned in the OP, but I remember getting it maybe 4 months back.

Aura - May 20, 2014, 2:14 pm

(May 20, 2014 02:13 PM)?Infamy Wrote: [\[CITE\]](#) It's been on Skype for quite some time actually, I'm pretty sure it was originally for Skype and this Facebook version is a new strain of it.

The Skype message was the same type of thing that you mentioned in the OP, but I remember getting it maybe 4 months back.

The article mention that it's a new variant of another malware (Zusy Trojan), so I guess that might be it.

ZuGgY - May 20, 2014, 2:16 pm

Thanks for the heads up.

That is pretty idiotic if you open it up. ?

grady - May 20, 2014, 2:36 pm

(May 20, 2014 02:16 PM)ZuGgY Wrote: [\[CITE\]](#) Thanks for the heads up.

That is pretty idiotic if you open it up. ?

For people who know what's out there, it's idiotic.

For the average computer user, it's a friend sending them a picture.

Daxe - May 20, 2014, 2:54 pm

I feel like if I am at the point where I feel I should run in a VM or sandbox I probably shouldn't run it at all. Kaspersky Reputation FTW.

Aura - May 20, 2014, 3:09 pm

(May 20, 2014 02:54 PM)Daxe Wrote: [\[CITE\]](#) I feel like if I am at the point where I feel I should run in

a VM or sandbox I probably shouldn't run it at all. Kaspersky Reputation FTW.
Kaspersky is love, Kaspersky if life buddy.
This is the universal truth.

Dr. Manhattan - May 20, 2014, 3:10 pm

(May 20, 2014 03:09 PM)Aur? Wrote: [\[CITE\]](#) Kaspersky is love, Kaspersky if life buddy.
This is the universal truth.
Kaspersky is so OP ! I love to death that antivirus :)

Still, is there a way to remov that nasty thing from the pc's? I would love to help my buddy's out :/

Aura - May 20, 2014, 3:13 pm

(May 20, 2014 03:10 PM)Dr. Manhattan Wrote: [\[CITE\]](#) Kaspersky is so OP ! I love to death that antivirus :)

Still, is there a way to remov that nasty thing from the pc's? I would love to help my buddy's out :/
I don't remember the EXACT procedure SPECIFIC to that malware since when I do a clean-up, I go all the way and remove everything at once but my normal clean-up procedure got rid of it.

b?xxy - May 20, 2014, 3:14 pm

Thanks for this post OP! I've gotten a few of these, but I never click links >.> ?

Aura - May 20, 2014, 5:35 pm

(May 20, 2014 03:14 PM)BlackVeilBrides Wrote: [\[CITE\]](#) Thanks for this post OP! I've gotten a few of these, but I never click links >.> ?
No problem buddy, stay safe and continue not clicking random links ?

Jagster™ - May 22, 2014, 7:29 am

(May 20, 2014 02:36 PM)?Infamy Wrote: [\[CITE\]](#) For people who know what's out there, it's idiotic.
For the average computer user, it's a friend sending them a picture.
Yah this. Most people are not aware of the potential risks out on the web especially if its one of their "friends" sending them a file.

He B TeMy - May 23, 2014, 10:24 am

But tell me something, the file may be named ".zip" but when you download it, the browser especifically show's the file extension or am i wrong?
I know some web hosts don't show the extension, but all browsers do?

Just asking.

Aura - May 23, 2014, 11:03 am

(May 23, 2014 10:24 AM)HeBTeMy Wrote: [\[CITE\]](#) But tell me something, the file may be named ".zip" but when you download it, the browser especifically show's the file extension or am i wrong?
I know some web hosts don't show the extension, but all browsers do?

Just asking.

They show the extension but someone can think "Oh he sent the picture in a .zip file because it was too big or something". Also, a lot of people wouldn't understand why it's fishy to get a .zip file for a picture.

He B TeMy - May 23, 2014, 4:42 pm

(May 23, 2014 11:03 AM)Aur? Wrote: [\[CITE\]](#) They show the extension but someone can think "Oh he sent the picture in a .zip file because it was too big or something". Also, a lot of people wouldn't

understand why it's fishy to get a .zip file for a picture.

Oh, sorry, i misread your OP, i thought you typed "they download a jar file which shows only as .zip if you have that setting disabled." that's why i asked if the browser didn't show the file real extension... i should re-read before i post..

Now i understand what you said, :)

whitey0ext - May 23, 2014, 5:36 pm

(May 20, 2014 12:45 PM)RedSpyGentlemen Wrote: [\[CITE\]](#) Sometimes I download those on purpose to see what it will do.

I run it in sandboxie.

Lol never thought of this imma try it ?

Aura - May 23, 2014, 9:52 pm

(May 23, 2014 04:42 PM)HeBTMy Wrote: [\[CITE\]](#) Oh, sorry, i misread your OP, i thought you typed "they download a jar file which shows only as .zip if you have that setting disabled." that's why i asked if the browser didn't show the file real extension... i should re-read before i post..

Now i understand what you said, :)

They download a .zip that have a file that looks like a .png but is in reality a .jar because they'll name it "picture.png.jar" and if you have the "Hide file extensions for known extensions type" you'll see "picture.png" and it will be normal to you but it's in fact a .jar.

Haste. - May 23, 2014, 9:55 pm

Thanks for the alert, Aura. I appreciate it. I will make sure to be on the lookout for any infected friends.

Borzoi - May 23, 2014, 9:55 pm

Aura how do you know so much man!?!

Thanks for the update though, I don't use Facebook but that is interesting.

mrpopsikle - May 23, 2014, 9:56 pm

Thanks for the info Op but i never download shit off facebook anyway lol

Aura - May 23, 2014, 9:59 pm

(May 23, 2014 09:55 PM)Haste. Wrote: [\[CITE\]](#) Thanks for the alert, Aura. I appreciate it. I will make sure to be on the lookout for any infected friends.

No problem Haste and yes, I'm sure at least one of them is infected by now due to this malware spreading really fast.

(May 23, 2014 09:55 PM)Borzoi Wrote: [\[CITE\]](#) Aura how do you know so much man!?!

Thanks for the update though, I don't use Facebook but that is interesting.

Look in the OP for the source ?

(May 23, 2014 09:56 PM)mrpopsikle Wrote: [\[CITE\]](#) Thanks for the info Op but i never download shit off facebook anyway lol

It will be sent by one of your friend via Facebook chat, not from a Facebook post.

Bobby Trill - May 23, 2014, 9:59 pm

Wow , thanks for informing me about this ! Will look out for other people who do get something weird like this .

Aura - May 26, 2014, 7:16 pm

(May 23, 2014 09:59 PM)Macmillerr2011 Wrote: [\[CITE\]](#) Wow , thanks for informing me about this ! Will look out for other people who do get something weird like this .

A lot of people that just knows how to use a computer for school and web browsing will fall for it, so be careful to warn these people ?

Aceman - May 28, 2014, 7:25 am

I remember getting infected from this back when I was 13 on MSN, thanks for the heads up Aura ?.

Aura - May 28, 2014, 4:47 pm

(May 28, 2014 07:25 AM)Aceman Wrote: [\[CITE\]](#) I remember getting infected from this back when I was 13 on MSN, thanks for the heads up Aura ?.

Yeah, stupid spamming messages everywhere.

HIGH PAID FELLA - July 15, 2014, 11:58 am

(May 28, 2014 04:47 PM)Aur? Wrote: [\[CITE\]](#) Yeah, stupid spamming messages everywhere.

When I was 12 i was scared if somebody sent a .gif that states its loading a virus LOOOL.

Erwin Schrödinger - July 15, 2014, 12:01 pm

Thanks for the warning!

Is this like the virus that spread through Skype like wildfire?

Like one day did I get over 100 PM's asking me to download it.

I just sat in a corner, scared. :S

Aura - July 15, 2014, 12:04 pm

For your information, that malware has been taken down by Facebook :

<https://hackforums.net/showthread.php?tid=4331992>

Roger Waters - July 15, 2014, 3:20 pm

It has become more and more common for people to sell their facebook pages (actual pages that you can Like, not send friend requests to like a personal account) after they reach a certain amount of likes and a following that has people interacting with their posts. If you think about it, it is a great way to spread malware and stuff if you are into that kind of thing. People won't expect it from a popular facebook page and often don't notice the outcome from clicking on a link that a page has posted or a link on a post that someone has shared to their timelines.

Aura - July 15, 2014, 6:05 pm

(Jul 15, 2014 03:20 PM)Roger Waters Wrote: [\[CITE\]](#) It has become more and more common for people to sell their facebook pages (actual pages that you can Like, not send friend requests to like a personal account) after they reach a certain amount of likes and a following that has people interacting with their posts. If you think about it, it is a great way to spread malware and stuff if you are into that kind of thing. People won't expect it from a popular facebook page and often don't notice the outcome from clicking on a link that a page has posted or a link on a post that someone has shared to their timelines.

Are there members here doing that ? Like, making Facebook pages popular, or Facebook profile have a lot of followers and then coming on HackForums to sell these after ?

Roger Waters - July 15, 2014, 6:31 pm

(Jul 15, 2014 06:05 PM)Aur? Wrote: [\[CITE\]](#) Are there members here doing that ? Like, making Facebook pages popular, or Facebook profile have a lot of followers and then coming on HackForums to sell these after ?

I've seen people post sales threads selling facebook pages before, so I wouldn't be surprised if people did this. People buy fake followers and likes so they can expand their page, I wouldn't be

surprised if people get a few suckers to like their fake page and get some people infected thinking that they are clicking on a legit thing.

Aura - July 16, 2014, 3:34 am

(Jul 15, 2014 06:31 PM)Roger Waters Wrote: [\[CITE\]](#) I've seen people post sales threads selling facebook pages before, so I wouldn't be surprised if people did this. People buy fake followers and likes so they can expand their page, I wouldn't be surprised if people get a few suckers to like their fake page and get some people infected thinking that they are clicking on a legit thing.

True, Social Media shops are a gold mine here, with followers, likes, shares, etc. you can transform your Facebook page, Twitter tag, Youtube video in pretty much everything. And this is one of the most dangerous spreading method there is in my opinion because people follow what is popular, and when something is popular, they think that it's "trusted".