

Forum:[Hack Forums](#)

Thread: [Exploit.IM is malicious, please stop using it \(or at least read this first\)!](#)

Emoticon - July 17, 2015, 2:31 am

I'd like to take this final moment before going to sleep (hopefully) for the night to address something that I feel very strongly about. exploit.im's Jabber service.

There is no TL;DR or summary to what I have to say below. Either read it or don't.

I suppose it would be appropriate to start out by introducing its owner, Ivan Baskov, also known as Dest31337. Ivan attempts to attack everyone who targets his XMPP service. He feels very strongly about his ability to scam and otherwise con people while communicating securely with his partners in crime through his XMPP service. Somewhat recently, somebody attacked and hijacked his domain. I'm hearing that there was a database leak for this service, but I haven't been able to confirm it. While he somewhat quickly responded to the attack, it seems that he learned the power he could claim by leaving the security standards similar to how they were when the service was compromised. This lead to how it is today.

Today, exploit.im is still fairly active (especially among a community of teenagers who want to fit in and look like 1337 h4x0rs.) What they don't realize is that any non-OTR conversations are being logged and scanned for any sensitive information, and that their passwords are being stored in clear-text format (meaning the administrators can see your password). Generally the first message of a conversation is the most likely to be left unencrypted, because "automatic OTR" waits for the first message at times. Anything that looks remotely sensitive can and will be used against you by the service's administrator(s).

Yesterday, I saw that Rory Guidry (also known as KMS, Agent KMS, and Rory Andrew Godfrey [pseudonym]) was arrested in the multinational Darkode takedown operation. His username on Darkode was "k@exploit.im", and many of the chat logs that were recovered and could potentially be used against him are from XMPP via exploit.im.

This next bit is a little more personal to me, and is actually one of the primary reasons (apart from what is mentioned in the above paragraph) why I am writing this out to everyone. Being an XMPP service administrator is not easy, you deal with many frauds and scammers attempting to use your service as a safe haven. The idea behind my service is dead-set privacy. No IP logging (except in special security occasions), absolutely no message stanza logging of any form.

This became very difficult when I was contacted by the primary administrator of the Exploit.IM service, Ivan. I do not speak fully fluent Russian, because I have not spoken it in quite a few years. I preferred my Russian over his English, since it made no sense. We exchanged messages, and apparently one of my service's users was harassing his friend. He wanted me to give up logs on the user, threatened to "root" (compromise) my services to obtain what he wanted. Obviously I declined, even had I accepted there was no information to hand over.

This is when the attacks begun.

At first it was just a few registrations a day, which I noticed due to flood flags in the security audit log. I thought nothing of it. Next thing I knew, every single one of the accounts was spamming a single user of the xmpp.jp service. At this point I realized that my service had just become a vector

for somebody's denial of service attack against the xmpp.jp service (which I respect). Instantly I put the service in rate-limiting mode. One message a minute. Any users here that use my service may have experienced that for the hour it was activated, but I wouldn't count on it.

Once I found and unregistered the accounts involved in the attack (over 100), I turned my attention to prevention of future attacks. For weeks, any countermeasure I would put in place the attacker would circumvent it. At one point the primary goal of the attack was to fill up hard drive space (logs) and consume CPU resources (which actually caused slightly noticeable service-wide lagging). This attack was launched using error stanzas, which weren't blocked by my countermeasures (at the time).

For over two weeks, I had to worry about my free privacy-oriented XMPP service being attacked by somebody who was clearly associated with Baskov. I spoke to him again and taunted him a little bit, so he obviously hired somebody to take down my XMPP service with a layer 4 (UDP with what seems to be a CHARGEN amplification) attack. Since I was, at the time, using direct [censored] connection for my XMPP service, it went down rather quickly. I have since added DDoS filtering.

Exploit.IM has caused me a lot of problems, and after reading this I hope you understand that it has the potential to cause you a lot of problems as well. Please take this into consideration when registering or advertising your JID.

Since I'm talking about XMPP, I might as well mention that my XMPP service is open and available for registration. I don't spy on you or compromise your security for my personal gain like Baskov does. Read up on it here: <https://xor.li/>

Obviously, if anyone has any questions or comments, you can reply here. A more private method of contacting me would be to add me as a contact on XMPP/Jabber. My JID is h@xor.li.

Thanks for reading.

HIGH PAID FELLA - July 17, 2015, 2:37 am

True, exploit.im has been compromised multiple times.

The best option would be hosting your own server like in my signature and yours.

Emoticon - July 17, 2015, 2:40 am

(Jul 17, 2015 02:37 AM)Asterea Wrote: [CITE](#) True, exploit.im has been compromised multiple times. The best option would be hosting your own server like in my signature and yours.

I, as well, feel that it's best for everyone to run their own service; however, a lot of people who are seeking secure, private communication options are not capable of correctly configuring a service on their own. It seems these are the types of people who gravitate toward services like exploit.im, since they come off as being "cool" and "hackerish"... sadly that deception is what may have cost Rory Guidry many years of his life.

~Jay~ - July 17, 2015, 8:12 am

I never understood why people trust chat/e-mail providers. If I ever have anything sensitive that needs to be said/transmitted I ALWAYS encrypt it with a private key. I can't fathom why I always hear about "famous" blackhats getting charged because of unencrypted chat logs. They should know best of all how vulnerable sites/services run by others are.

If it's run by anyone besides yourself or encrypted by anyone besides yourself, don't trust it.

rudeman - July 17, 2015, 8:18 am

i used exploit.im for the exact reason op states, this was a year ago though, any passwords of mine

which (were) allegedly stolen were already in public databases, i read through all and i'm sorry you were targeted

Tony S - July 17, 2015, 10:07 am

Good write-up.

I have heard nothing but negativity about exploit.im ever since its inception. Given the history of the service (and I use the term "service" very lightly) and the reputation of Mr. Baskov, I see no reason as to why anyone should continue using the obviously corrupt service.

Also, good luck with your Podso project.

R3FACTOR - July 17, 2015, 10:38 am

Thanks this clears up a lot, I kept reading everywhere that people don't recommend exploit.im. I didn't know what was wrong with it. Thanks OP.

ZuGgY - July 17, 2015, 10:41 am

Lol, I never used it, never will. It's a stupid XMPP service.

sinmar - July 17, 2015, 11:18 am

Pretty much all XMPP service admins spy on their users and attack eachother. If you use a public XMPP service expect to be monitored and used as a pawn when needed.

CRAIG XEN - July 17, 2015, 4:57 pm

I was on Darkode way back in the day, Sp3c regularly paid Dest31337 for logs and plaintext PW's that Dest31337 keeps.

The thing is all the kids here have no fucking clue about whats up with exploit.im and use it because it looks cool.

I still reccomend jabber.calyxinstitute.org.

John Constantine - July 18, 2015, 3:30 am

People that have the chance to use the HF XMPP should use it, this requires OTR.

Tony S - July 18, 2015, 5:05 am

(Jul 18, 2015 03:30 AM)Phil Coulson Wrote: [\[CITE\]](#) People that have the chance to use the HF XMPP should use it, this requires OTR.

hackforums.im runs on a closed network. You can only communicate with others that have a hackforums.im account (which I believe requires you to be upgraded) - no other server.

It's pretty useless to myself and many others.

Emoticon - July 19, 2015, 9:04 pm

(Jul 17, 2015 04:57 PM)Hunger Wrote: [\[CITE\]](#) I was on Darkode way back in the day, Sp3c regularly paid Dest31337 for logs and plaintext PW's that Dest31337 keeps.

The thing is all the kids here have no fucking clue about whats up with exploit.im and use it because it looks cool.

I still reccomend jabber.calyxinstitute.org.

I had no idea they were associated, that makes matters much worse than I had originally thought.

I can't say I'm very surprised, however.

I can also confirm that Dest31337 is still active, he has been trying to cause me problems this weekend.

(Jul 17, 2015 11:18 AM)sinmar Wrote: [\[CITE\]](#) Pretty much all XMPP service admins spy on their users and attack each other. If you use a public XMPP service expect to be monitored and used as a pawn when needed.

I can agree with this for the most part. I do feel that some service administrators are still good and actually care about running a service to reinforce the privacy of its users, but you can never know who is being honest. I can say a million times that I respect my users' privacy, but that doesn't make it believable.

lvps - July 21, 2015, 6:41 pm

The XMPP server exploit.im is backdoored along with jabber.se

jazzy1047 - July 21, 2015, 6:42 pm

Hi

Can your please brief me on this program, i have heard so much about this topic

please brief me

hope to hear from you soon.

thank you very much

Greeatest

Infinity. - July 25, 2015, 4:38 pm

I am currently using creep.im, mainly to talk to 2-3 friends I made offsite. That's pretty sad that it happened to you. Goodluck man.

<https://xmpp.net/result.php?domain=creep.im&type=client>

Any opinions on it?

Epicur - December 16, 2015, 7:11 am

Thanks for the info, I will stop using exploit.im.

The name is really cool though :(

Athanatos - December 16, 2015, 7:18 am

Thanks for the info, but its pretty obvious Sp3c OF DARK0DE was a fed.

Crowsnest - December 16, 2015, 2:44 pm

Thanks for the heads up, I'll keep this in mind.

I used to use exploit.im, looks like I won't be doing that again.

Epicur - December 16, 2015, 2:56 pm

I'm using dukgo.com now as a XMPP server, any thoughts or information about it that I don't know? I have googled it and it seems pretty secure, anyone has something against it?

Sorry for going off-topic and thanks!

LordHello - *December 16, 2015, 3:08 pm*

Just created an xor.li xmpp.

Thanks for this OP!

usafety - *April 8, 2021, 2:31 am*

exploit.im is down since 2 weeks, maybe they got busted?