

Forum:[Hack Forums](#)

Thread: [doing a research project on Blackshades](#)

wit - October 30, 2017, 9:29 am

For my comp forensics class, i'm doing a 5 page research project on Blackshades.
Is Wikipedia the most extensive source to use?
Would HF be a credible source?

if anyone knows any extra information on Blackshades, xvisceral, anything really i'd really appreciate it

SIM-1589588 - October 30, 2017, 9:32 am

I think you should contact BV1 (Twitter @BV1tech) and Farhan (Indecisive enough) to get more background information.

wit - October 30, 2017, 9:34 am

(Oct 30, 2017 09:32 AM)J.P Morgan Wrote: [\[CITE\]](#) I think you should contact BV1 and Farhan (Indecisive enough) to get more background information.
BV1 seems to be banned (idk why) and Farhan i will definitely reach out to.

Thanks

SIM-1589588 - October 30, 2017, 9:36 am

(Oct 30, 2017 09:34 AM)CydiaDev Wrote: [\[CITE\]](#) BV1 seems to be banned (idk why) and Farhan i will definitely reach out to.

Thanks

You can contact BV1 on his twitter, he's still active there. Twitter @BV1tech

canine - October 30, 2017, 9:38 am

(Oct 30, 2017 09:34 AM)CydiaDev Wrote: [\[CITE\]](#) BV1 seems to be banned (idk why) and Farhan i will definitely reach out to.

Thanks

BV1 is back on the forums on a new acc iirc

I doubt HF would be a credible source. Reminds me of the time my friend was using Evangelion as a source for some existentialism paper he was writing. His professor gave him an alright grade because it was obvious he understood what he was writing about in the paper, but he couldn't really give much for source material. Friendly reminder to not let your college professors know you watch anime.

lwristis - October 30, 2017, 9:42 am

u could use the arrest warrant they had for xvis, heard about the raid in irc was a spooky moment

GenericSkid - October 30, 2017, 9:45 am

I mean, it was a HF product. That makes HF as close to a primary source as you can get. I'm sure somebody on here has a story to tell. You can for sure PM the people who made threads saying they got raided for using it.

SIM-1589588 - October 30, 2017, 9:46 am

Don't forget to include Alex (Marjinz) in your project because he's the one who coded that shit and scammed hundreds of people by promising them silent exploit.

lwrist - October 30, 2017, 9:47 am

(Oct 30, 2017 09:45 AM)GenericSkid Wrote: [\[CITE\]](#) I mean, it was a HF product. That makes HF as close to a primary source as you can get. I'm sure somebody on here has a story to tell. You can for sure PM the people who made threads saying they got raided for using it. was it a hf product? i remember talking to michael he mentioned hf, but never mentioned it being an exclusive hf product?

SIM-1589588 - October 30, 2017, 9:50 am

I found something for you.

<https://www.dropbox.com/s/pfdzrmczbwabjji/Blackshades%20-%20My%20services.pdf>

some more details

<https://hackforums.net/showthread.php?tid=3769093>

(Oct 30, 2017 09:47 AM)oxid Wrote: [\[CITE\]](#) was it a hf product? i remember talking to michael he mentioned hf, but never mentioned it being an exclusive hf product?

If I'm not wrong and my memory is correct, it was being exclusively sold on hackforums and their official website. There used to be a special subforum.

<https://hackforums.net/showthread.php?tid=2623715>

lwrist - October 30, 2017, 9:56 am

On their website would mean it wasn't exclusive to this site...

xvis was a hard working guy didn't deserve that "top 9 cyber-terrorist" shit

wit - October 30, 2017, 12:37 pm

(Oct 30, 2017 09:50 AM)J.P Morgan Wrote: [\[CITE\]](#) I found something for you.

<https://www.dropbox.com/s/pfdzrmczbwabjji/Blackshades%20-%20My%20services.pdf>

some more details

<https://hackforums.net/showthread.php?tid=3769093>

If I'm not wrong and my memory is correct, it was being exclusively sold on hackforums and their official website. There used to be a special subforum.

<https://hackforums.net/showthread.php?tid=2623715>

how u found that dropbox link is insane

good stuff my man thank u +3

SIM-1589588 - October 30, 2017, 1:01 pm

Found one more good pdf about blackshades.

<http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-blackshades-rat.html>

Tony Stark - October 30, 2017, 1:17 pm

Anyone who actually knows anything, won't be stupid enough to post.

Inb4 this is a trap, good luck on the paper ;) ;)

wit - October 30, 2017, 2:57 pm

(Oct 30, 2017 01:17 PM)Tony Stark Wrote: [\[CITE\]](#) Anyone who actually knows anything, won't be stupid enough to post.

Inb4 this is a trap, good luck on the paper ;) ;)
bruh do u wanna see the syllabus

fuck u think i am calling me a snitch

im not looking for top tier info jus a general basis of how they were caught

Cooligan - October 30, 2017, 4:09 pm

Now that's an interesting choice for a school project.

wit - October 30, 2017, 7:19 pm

(Oct 30, 2017 04:09 PM)Cooligan Wrote: [\[CITE\]](#) Now that's an interesting choice for a school project. we had to choose a malware/hack and equifax/ashley madison seemed too normie

plus i was kinda hoping bv1 would respond to my PMS but hes banned :(

Armada - October 30, 2017, 7:24 pm

(Oct 30, 2017 09:38 AM)w342 Wrote: [\[CITE\]](#) BV1 is back on the forums on a new acc iirc

I doubt HF would be a credible source. Reminds me of the time my friend was using Evangelion as a source for some existentialism paper he was writing. His professor gave him an alright grade because it was obvious he understood what he was writing about in the paper, but he couldn't really give much for source material. Friendly reminder to not let your college professors know you watch anime.

Why in the hell would Hack forums not be a credible source for info?

The damn software originated on here and spread out from there.

Also many members including myself were customers of the software, no better place to get first hand accounts from people who actually used the software.

wit - October 30, 2017, 7:27 pm

(Oct 30, 2017 07:24 PM)Armada Wrote: [\[CITE\]](#) Why in the hell would Hack forums not be a credible source for info?

The damn software originated on here and spread out from there.

Also many members including myself were customers of the software, no better place to get first hand accounts from people who actually used the software.

these were my thoughts exactly

i assumed original customers/devs would still be lurking around here

canine - October 30, 2017, 7:31 pm

(Oct 30, 2017 07:24 PM)Armada Wrote: [\[CITE\]](#) Why in the hell would Hack forums not be a credible source for info?

The damn software originated on here and spread out from there.

Also many members including myself were customers of the software, no better place to get first hand accounts from people who actually used the software.

As far as I'm concerned HF isn't a credible source for drama like this because of all of the misinformation spread by retards on this site but I get what you're saying. Regardless it probably wouldn't be a credible source of information to a professor and that's all that matters in this situation. Teachers and professors can be assholes with what you use to cite sources or they could be pretty down to earth.

Armada - October 30, 2017, 7:34 pm

(Oct 30, 2017 07:31 PM)w342 Wrote: [\[CITE\]](#) As far as I'm concerned HF isn't a credible source for drama like this because of all of the misinformation spread by retards on this site but I get what you're saying. Regardless it probably wouldn't be a credible source of information to a professor and that's all that matters in this situation. Teachers and professors can be assholes with what you use to cite sources or they could be pretty down to earth.

Maybe true, If I were OP I'd focus 3/4 of the paper on the technical and logistics and use and on site HF sources/resources as kinda like icing on the cake.

But that's just my opinion.

@OP, Do not forget to cover the fact the FBI had Main dude (Alex was it?) backdoor the software to nab all the customers. They really try to down play that part but its in the documents....

SIM-925118 - October 30, 2017, 7:55 pm

<https://archives.fbi.gov/archives/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown>

Cagey - October 30, 2017, 8:40 pm

I know a fed busted one of the guys for carding he was teaching the fed how to card obviously didnt know he was a fed

GenericSkid - October 30, 2017, 9:06 pm

(Oct 30, 2017 07:24 PM)Armada Wrote: [\[CITE\]](#) Also many members including myself were customers of the software,
Knock knock, its the feds!

Armada - October 30, 2017, 9:11 pm

(Oct 30, 2017 09:06 PM)GenericSkid Wrote: [\[CITE\]](#) Knock knock, its the feds!
They have the database, and I use my regular email for registrations.

Think they of all people do not know? ?

No one knocked on my door, funny how that went, Shit I bought using Paypal too. lol

Neal Caffrey - October 31, 2017, 7:10 pm

(Oct 30, 2017 09:42 AM)oxid Wrote: [\[CITE\]](#) u could use the arrest warrant they had for xvis, heard about the raid in irc was a spooky moment
confirmed multiaccounter you've been reported kid

wit - November 2, 2017, 2:10 pm

(Oct 30, 2017 07:55 PM)Albatraoz Wrote: [\[CITE\]](#)
<https://archives.fbi.gov/archives/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assis>

[tant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown](#)

thank you, i could use more sources like this.

For anyone thinking im a fed/this is fake:

dat boi - November 2, 2017, 2:11 pm

If I used wikipedia for a source, my professor would shove a comma splice in my arse.

wit - November 2, 2017, 6:23 pm

(Nov 2, 2017 02:11 PM)dat boi Wrote: [\[CITE\]](#) If I used wikipedia for a source, my professor would shove a comma splice in my arse.

the key is to use wikipedia then jus use the sources they list in the bottom

\$ZEUS - November 3, 2017, 9:36 am

Don't forget to include the lack of personal security these idiots do to even show they care about freedom. You can have the biggest RAT on the market, and still be the biggest fucking idiot because you don't know about personal security.

lucky. - November 3, 2017, 12:05 pm

If you source something like the sales threads I'm sure it would be credible, but at the same time you'll want to find the sales threads of their CC fraud (if its still out there) since that was a major part of it.

Generating - November 4, 2017, 10:46 pm

I've got a old YouTube video like 5 years ago of someone using Blackshades to rat my PC. Basically, he ratted me and then uploaded a video to my YouTube channel of him and all of his clients. You could show the video in your presentation so people have a visual representation of what you mean when you talk about it.

Bluffer - November 4, 2017, 10:48 pm

Also you should use the FBI reports about the investigations in your project.

test - November 4, 2017, 10:49 pm

BV1 might be happy to talk to you. I don't know the extent of information you'll get out of him but he's a nice guy. He more than likely has another account but if you need help reaching him just let me know.

Crya - November 4, 2017, 11:45 pm

Why is BV1 banned on his new account?

test - November 4, 2017, 11:48 pm

(Nov 4, 2017 11:45 PM)Crya Wrote: [\[CITE\]](#) Why is BV1 banned on his new account?

He abused the rep bumping feature when HF was first upgraded to 1.8.

Butane - November 4, 2017, 11:49 pm

Search up on google and there's a lot of tech article about that like kreb and some antivirus blog. They can also be your reliable source too.

Deutsche Bank - November 5, 2017, 3:37 am

<https://hackforums.net/member.php?action=profile&uid=3183372>

BV1's new account.

too bad hes banned again lmao

just tweet at him on twitter, he will reply.

wit - November 5, 2017, 10:12 am

(Nov 4, 2017 10:49 PM)testaccountplsignore Wrote: [\[CITE\]](#) BV1 might be happy to talk to you. I don't know the extent of information you'll get out of him but he's a nice guy. He more than likely has another account but if you need help reaching him just let me know.

im gonna try his twitter and if he doesn't hmu there ill gladly take u up on that

I'm not looking for top secret information, just 2 questions i can write about:

1. What was the main goal for BS
2. How did they get caught

Nomad.Null - November 5, 2017, 3:54 pm

If you want a credible source for Blackshades, what better place than the investigation files?

<https://www.fbi.gov/news/stories/international-blackshades-malware-takedown-1>

Plenty of additional citations at the bottom of this page ^

Kr3bz also did a bit on it, but his name is taboo here so I'm not even allowed to say it XD

I was around for the Blackshades takedown but never had the software in my hands. Honestly, it wasn't very forensically difficult to uncover its source from what I've understood. You could probably find snippets of the source code on github if you looked around.

(Nov 5, 2017 11:12 AM)CydiaDev Wrote: [\[CITE\]](#) im gonna try his twitter and if he doesn't hmu there ill gladly take u up on that

I'm not looking for top secret information, just 2 questions i can write about:

1. What was the main goal for BS
2. How did they get caught

The Blackshades group got caught because the primary developer and leader of the group got busted and struck a deal with the FBI. This I remember very clearly. The story was that he agreed to backdoor the software which was used by the FBI to take down most of the most significant users of the RAT. Once it got out that the RAT was backdoored, people started zero-filling hard drives faster than the FBI could drive to their houses to arrest them. There weren't many convictions, but it did send a message, in the FBI's usual fashion, that they had a boot ready to stomp on every hacker's neck that dared pick up a piece of malware regardless of intent or usage.

wit - November 17, 2017, 7:59 am

bump starting this project today any links would be a blessing

Armada - November 17, 2017, 8:53 am

(Nov 5, 2017 04:54 PM)True Demon Wrote: [\[CITE\]](#) The Blackshades group got caught because the primary developer and leader of the group got busted and struck a deal with the FBI. This I remember very clearly. The story was that he agreed to backdoor the software which was used by the FBI to take down most of the most significant users of the RAT. Once it got out that the RAT was

backdoored, people started zero-filling hard drives faster than the FBI could drive to their houses to arrest them. There weren't many convictions, but it did send a message, in the FBI's usual fashion, that they had a boot ready to stomp on every hacker's neck that dared pick up a piece of malware regardless of intent or usage.

Fucking THIS

If you want a first hand account from a customer shoot me a PM OP

wit - November 17, 2017, 9:06 am

(Nov 17, 2017 09:53 AM)Armada Wrote: [\[CITE\]](#) Fucking THIS

If you want a first hand account from a customer shoot me a PM OP
thanks man, imma send you a PM now.

NoneStar - November 17, 2017, 9:11 am

(Oct 30, 2017 08:40 PM)Calisthenics Wrote: [\[CITE\]](#) I know a fed busted one of the guys for carding he was teaching the fed how to card obviously didnt know he was a fedDang, never knew that about the carding thing, always thought they just got caught, not that they taught someone how to do it.

Deus_ - November 17, 2017, 9:31 am

You better not, I lost my good old computer because of BS D:

Police stole it :(