

Forum:[Hack Forums](#)

Thread: [Found databreach contacted the company](#)

Phased - October 9, 2018, 5:22 pm

Once in a while I check my shodan plugin, while i was reading the site i noticed the shodan popup which stated that port: 21 (For the <12yo peeps: FTP " File Transter Protocol"). I wonder why this is still being used anyway...

While making connection without any creds, i obtained access to the domain FileServer ? what a epic fail...

Litterly everything was just there i started wondering if this wasnt some honey pot or somethin (There are a lot ot them out there).. littlerly in the root / directory ALL files were available even automounting scripts for Windows hosts.

The ACL was just not configured i guess on their Domain, i saw tons of ID's, HR Salaryslips, Private company data, Proposals towards other companies and many many more stuff like 10TB of HQ Pr0n *Just kidding" ?

I havent tried to write to the server as i noticed that there were not even XMR Miners placed in every folder+subfolder (image.csr). Perhaps i was only able to read and not to write.

Then I immediatly contacted the company, got forward on the phone... then on HOLD,.... aaaaand forwarded, jesus took some time until i finally had the general boss on the phone.

He wanted to provide me some screenshots (which i offcourse already made! I mean thats just what pentesters do making screenshots and wirting notes like crazy). At the same moment during my call my FTP session got disconnected. I bet they somehow knew about the breach... So i told him that i'll sent him a report of my findings and avisory but also that he might have to report to the Authorities due to the data protection law. I think a full fresh data-breach can be very profitable when selling on some shady location. But from an ethical perspective (whitehat) i would never do something like that.

His last words were, Thanks you and if you can find more let me please know.

Sirously?? (I'm don't care much about hacker swag or whatever), but at least he could have proposed something and now he thinks im going to do further reasearch on webapp testing?? FORE FREE? c'monn

Joking:

So who wants to buy data? Time to go ?

DON'T PM ME ABOUT THIS, ITS AGAIN A JOKE AND I'M NOT INTERSTED IN ANY BLACKHAT RELATED WORK... thank you

Anyway just annoying that some companies just don't give a f*ck about (our) data publicly available.

I think I will call the director again and have a nice chat with hime

- Z - - October 9, 2018, 5:25 pm

LMAO, Tell me why i read the whole thing and actually thought it was real till the end, Nice story

SIM-3257834 - October 9, 2018, 5:27 pm

You should send him this thread that way he'll know you're serious about a award because you're a

HF member.

Phased - October 9, 2018, 5:38 pm

(Oct 9, 2018 05:25 PM)- Z - Wrote: [\[CITE\]](#) LMAO, Tell me why i read the whole thing and actually thought it was real till the end, Nice story

Forgot to add but any advice? I'ts not a joke it was a huge leak, from an ethical perspective i would never leak private information. (Thats why i joked about selling the data).

I told him that there's a law and he have to report this incident, just feels like he doesnt care or he's just an idiot.

Maybe I should report this to the authorities myself? I mean just show some respect and be happy that i actually took the effort to call them and report it.

Mushin - October 10, 2018, 5:09 am

(Oct 9, 2018 05:22 PM)Phased Wrote: [\[CITE\]](#) Once in a while I check my shodan plugin, while is was reading the site i noticed the shodan popup which stated that port: 21 (For the <12yo peeps: FTP " File Transter Protocol"). I wonder why this is still being used anyway...

While making connection without any creds, i obtained access to the domain FileServer ? what a epic fail...

Litterly everything was just there i started wondering if this wasnt some honey pot or somethin (There are a lot ot them out there).. littlerly in the root / directory ALL files were available even automounting scripts for Windows hosts.

The ACL was just not configured i guess on their Domain, i saw tons of ID's, HR Salaryslips, Private company data, Proposals towards other companies and many many more stuff like 10TB of HQ PrOn *Just kidding" ?

I havent tried to write to the server as i noticed that there were not even XMR Miners placed in every folder+subfolder (image.csr). Perhaps i was only able to read and not to write.

Then I immediatly contacted the company, got forward on the phone... then on HOLD,.... aaaaand forwarded, jesus took some time until i finally had the general boss on the phone.

He wanted to provide me some screenshots (which i offcourse already made! I mean thats just what pentesters do making screenshots and wirting notes like crazy). At the same moment during my call my FTP session got disconnected. I bet they somehow knew about the breach... So i told him that i'll sent him a report of my findings and avisory but also that he might have to report to the Authorities due to the data protection law. I think a full fresh data-breach can be very profitable when selling on some shady location. But from an ethical perspective (whitehat) i would never do something like that.

His last words were, Thanks you and if you can find more let me please know.

Sirously?? (I'm don't care much about hacker swag or whatever), but at least he could have proposed something and now he thinks im going to do further reasearch on webapp testing?? FORE FREE? c'monn

Joking:

So who wants to buy data? Time to go ?

DON'T PM ME ABOUT THIS, ITS AGAIN A JOKE AND I'M NOT INTERSTED IN ANY BLACKHAT RELATED WORK... thank you

Anyway just annoying that some companies just don't give a f*ck about (our) data publicly available.

I think I will call the director again and have a nice chat with hime

Hi tried to send you a dm are you able to send/receive?

Strayaa - October 10, 2018, 5:15 am

(Oct 9, 2018 05:38 PM)Phased Wrote: [\[CITE\]](#) Forgot to add but any advice? I'ts not a joke it was a huge leak, from an ethical perspective i would never leak private information. (Thats why i joked about selling the data).

I told him that there's a law and he have to report this incident, just feels like he doesnt care or he's just an idiot.

Maybe I should report this to the authorities myself? I mean just show some respect and be happy that i actually took the effort to call them and report it.Nah bro leave it at that, don't call anyone just leave it. Sometimes its not worth going through all the effort

Good job on the find though! Can you tell me more about this plugin?

Phased - October 10, 2018, 6:48 am

(Oct 10, 2018 05:15 AM)STBG_banappeal Wrote: [\[CITE\]](#) Nah bro leave it at that, don't call anyone just leave it. Sometimes its not worth going through all the effort

Good job on the find though! Can you tell me more about this plugin?

Nothing fancy just the Shodan Firefox/Chrome plugin, so you can quickly check the services indexed by shodan on the site you currently visit.

(Oct 10, 2018 05:09 AM)Mushin Wrote: [\[CITE\]](#)

Hi tried to send you a dm are you able to send/receive?

Hmm should work according to my settings

Strayaa - October 10, 2018, 7:02 am

(Oct 10, 2018 06:48 AM)Phased Wrote: [\[CITE\]](#) Nothing fancy just the Shodan Firefox/Chrome plugin, so you can quickly check the services indexed by shodan on the site you currently visit.

Hmm should work according to my settings

was just playing with it before. check my recent threads. it's nice getting back in to this stuff lmao

Silent Uprising - October 10, 2018, 7:33 am

Well you broke the law. Shouldn't of been doing it in the first place.

I'm going to sound like a major dick, but I feel like I would of just kept quite about this. Although if I had the skills I would be a white hat...the reason I wouldn't report it is out of fear that after I help them out and telling them about a vulnerability, they might take me to court and charge me for hacking there DB.

kuzban - October 12, 2018, 3:35 am

(Oct 10, 2018 07:33 AM)Silent Uprising Wrote: [\[CITE\]](#) Well you broke the law. Shouldn't of been doing it in the first place.

I'm going to sound like a major dick, but I feel like I would of just kept quite about this. Although if I had the skills I would be a white hat...the reason I wouldn't report it is out of fear that after I help them out and telling them about a vulnerability, they might take me to court and charge me for hacking there DB.

Is it illegal, forgive my ignorance but isn't shodan legal and it just picks up on the data leaked by the company?

Rajj - October 12, 2018, 4:25 am

(Oct 10, 2018 07:33 AM) Silent Uprising Wrote: [\[CITE\]](#) Well you broke the law. Shouldn't of been doing it in the first place.

I'm going to sound like a major dick, but I feel like I would of just kept quiet about this. Although if I had the skills I would be a white hat...the reason I wouldn't report it is out of fear that after I help them out and telling them about a vulnerability, they might take me to court and charge me for hacking their DB.

This. It's fucked up but sometimes that's just how the law works. It's better to let things like this go sometimes.

kuzban - October 15, 2018, 4:57 am

(Oct 9, 2018 05:22 PM) Phased Wrote: [\[CITE\]](#) Once in a while I check my shodan plugin, while I was reading the site I noticed the shodan popup which stated that port: 21 (For the <12yo peeps: FTP "File Transfer Protocol"). I wonder why this is still being used anyway...

While making connection without any creds, I obtained access to the domain FileServer ? what a epic fail...

Literally everything was just there I started wondering if this wasn't some honey pot or something (There are a lot of them out there).. literally in the root / directory ALL files were available even automounting scripts for Windows hosts.

The ACL was just not configured I guess on their Domain, I saw tons of ID's, HR Salary slips, Private company data, Proposals towards other companies and many many more stuff like 10TB of HQ Pr0n *Just kidding" ?

I haven't tried to write to the server as I noticed that there were not even XMR Miners placed in every folder+subfolder (image.csr). Perhaps I was only able to read and not to write.

Then I immediately contacted the company, got forward on the phone... then on HOLD,.... aaaaand forwarded, Jesus took some time until I finally had the general boss on the phone.

He wanted to provide me some screenshots (which I of course already made! I mean that's just what pentesters do making screenshots and writing notes like crazy). At the same moment during my call my FTP session got disconnected. I bet they somehow knew about the breach... So I told him that I'll send him a report of my findings and advisory but also that he might have to report to the Authorities due to the data protection law. I think a full fresh data-breach can be very profitable when selling on some shady location. But from an ethical perspective (whitehat) I would never do something like that.

His last words were, Thanks you and if you can find more let me please know.

Seriously?? (I don't care much about hacker swag or whatever), but at least he could have proposed something and now he thinks I'm going to do further research on webapp testing??
FOR FREE? c'mon

Joking:

So who wants to buy data? Time to go ?

DON'T PM ME ABOUT THIS, ITS AGAIN A JOKE AND I'M NOT INTERESTED IN ANY BLACKHAT RELATED WORK... thank you

Anyway just annoying that some companies just don't give a f*ck about (our) data publicly available.

I think I will call the director again and have a nice chat with hime

Hey get me on jabber kaizen0006@jabbb3r.org I'm interested in knowing more