Get this straight…

September 11th, 2007 by admin | Posted in DEranged Security | 7 Comments »

#1 I'm not employed by any company, DEranged Security is the only source of this. All other titles are completely untrue if I'm not hired directly to do a job.

#2 ToR isn't bad! Every time you do anything unencrypted you are at risk even when you don't use ToR. When you put in a password on a site or log on a pop3 unencrypted your password can be stolen, you are sending it clear-text. You know nothing about who will be listening in and sometimes you don't even know anything about the site you are communicating with.

Time to reveal…

September 10th, 2007 by admin | Posted in DEranged Security | 62 Comments »

This is going to be a long post, several important things needs to be said. It's important you read it to the end.

We choose to wait this long before posting the whole story to give not only governments time to secure themselves but also to protect private users and businesses. The affected on the list has by now figured out that we had passwords to many more than just the 100 we posted and secured ALL their accounts. Many of the private/company users have by now received our e-mails warning them, few responses though. Remember that we found this kind of information on thousands of users, some of them being fortune 500 companies, Nasdaq and New York noted companies. The information we gathered is not worth millions, it's worth billions in the right hands. So anyone questioning my actions can go fuck yourself, I didn't make a penny of this except getting myself in trouble.

No accounts have been hacked, you have been actively exposing them yourself not only to us but to about 1000 others all over the world, every day. This has been told about many times before which you choose to ignore. The team behind the product is completely open with this security threat but they probably should have made a bigger warning text I guess. For us to publish yet another warning or for the vendor to tell you again would have gotten no effect once more.

We choose to publish 100 sensitive accounts for Governments in full disclosure to get heads turned. Remember that it still was thought of as a hoax from both users and admins everywhere until a crazy journalist in India started publishing stuff from some accounts. Posting parts of passwords and we would still be having denials and no actions today.

Did the account owners know about it? Of course they did! Most journalists had already talked to the embassies about the expose and got told that the security was fine and no one could know the passwords. This long before it started spreading and people starting using the accounts.

Having Governments all over the world working against me is fun to follow. Trying to pull focus away from themselves being idiots and over to me by using the term "hacker". The journalist loves that word and I see it more and more next to my name. I'm not a hacker and haven't broken into anything illegally. Whoever says that is welcome to prove it, probably easier to prove that I killed JFK. I'm a security specialist doing this stuff every day, always under controlled terms and completely legal. However being a bit DEranged I sometimes walk in the gray zone, exactly what it takes get stuff done. I fight criminals but when we have to play by the rules and they don't it's a tuff battle. Computer Crimes are real, they are everywhere and they are using your ignorance!

Alright, with the boring stuff said this is how we did it:

#1 Five ToR exit nodes, at different locations in the world, equipped with our own packet-sniffer focused entirely on POP3 and IMAP traffic using a keyword-filter looking for words like "gov, government, embassy, military, war, terrorism, passport, visa" as well as domains belonging to governments. This was all set up after a small experiment looking into how many users encrypt their mail where one mail caught my eye and got me started thinking doing a large scale test. Each user is not only giving away his/her passwords but also every mail they read or download together with all other traffic such as web and instant messaging.

Did you get it? These governments told their users to use ToR, a software that sends all your traffic through not one but three other servers that you know absolutely nothing about. Yes, two are getting encrypted traffic but that last exit node is not. There are hundreds of thousands ToR-users but finding these kinds of accounts was… hmm… chocking! The person who wrote the security policy on these accounts should reconsider changing profession, start cleaning toilets! These administrators are responsible for giving away their own countries secrets to foreigners. I can't call it a mistake, this is pure stupidity and not forgivable!

ToR isn't the problem, just use it for what it's made for.

#2. I'll have a lot of people to thank for helping me here, you all know who you are white-hats and friends out there. ToR has about 1000 nodes set up to handle exit-traffic (unencrypted). These are the servers all you traffic is going to be sent through. Of course you know everything about them, right? I had five running during this test that no one knew about, who owns the others?

Just to give you something to think about we did look into a few servers out of 1000 we thought looked interesting. We aren't trying to tell you what to think, you will have to do that yourself.

Example of Exit-nodes that can read your traffic:

- **Nodes named devilhacker, hackershaven…**
- **Node hosted by an illegal hacker-group**
- **Major nodes hosted anonymously dedicated to ToR by the same person/organization in Washington DC. Each handling 5-10TB data every month.**
- **Node hosted by Space Research Institute/Cosmonauts Training Center controlled by Russian Government**
- **Nodes hosted on several Government controlled academies in the US, Russia and around Asia.**
- **Nodes hosted by criminal identity stealers**
- **Node hosted by Ministry of Education Taiwan (China)**
- **Node hosted by major stock exchange company and Fortune 500 financial company**
- **Nodes hosted anonymously on dedicated servers for ToR costing the owner US$100-500 every month**
- **Node hosted by China Government official**
- **Nodes in over 50 countries with unknown owners**
- **Nodes handling over 10TB data every month**

We can prove all this but not the intentions of each server. They might be very nice people spending a lot of money doing you a favor but it could just as well be something else. We don't however think it's weird that Universities are hosting nodes, just that you need to be aware of it. Criminals, hackers and Governments are running nodes, why?

This experiment has proven another major problem regarding Computer Security. Even though I haven't broken into anything which people blame me for, it's obvious that laws for computer crimes

are problematic. Laws don't work over boarders but the Internet and the criminals do.

This world experiment has never been done before, what would happen if someone was DEranged enough to post a list completely public worth millions exposing Governments. We got this message out to at least 157 countries and billions of people in just a week. I'll have to say that even it if took 5 days to get 70% fixed that was fast compared to what I'm used to.

I would like to say special thanksto the people of India, Iran and Uzbekistan who has been extremely supporting. And fuck all of you who are filing police reports on me, you are idiots and are only proving that you haven't understood anything.

PS: Data and hard drive on each node is destroyed and I forgot everything somehow 

"There is no eeeeeeeeeeennnnnnnddddddd to the possibilites"

//D

Where did we go?

September 6th, 2007 by admin | Posted in DEranged Security | 8 Comments »

Our site got shut down and we stood there not knowing why, couldn't get any information from anyone. You aren't going to like the answer we just dug up.

*** American law enforcement officials requested DEranged Security to be taken down ***

Woho, we pissed the US of! But why? Millions of people have already read the story and tens of thousands have those passwords. Monsters don't go away when you close your eyes. Security by obscurity in its finest hour, staring the US law enforcment!

Suddenly we have something that is on everyone's mouth and getting security tightened all over the world from private to companies to governments and you go about this way? Do you have any reason for trying to stop this behavior? I've seen people saying that the US would be angry now that we forced foreign countries to tighten their security so NSA or whatever can't read their secrets any longer. To me it sounds like bullshit taken out of a bad book but after this silly little stunt I'm reconsidering. Is there any reason you DO NOT want people to secure their systems? Please, do go grab the server, of course I put copies there with secret stuff! Pathetic…

Well about the case… They only people on the list who has been willing to talk to me so far are Iran. A big gold medal to Iran! Very nice talking to you and I appreciate our chat greatly.

*** Ironic that suddenly Iran are the good guys and US the bad ones ***

Directly to the people in the security industry out there to clarify some stuff. There is no exploit to publish, no vendor to contact. This have been told about before with no reactions. Publishing it yet one more time wouldn't have changed crap. Even after publishing a full disclosure list like we did, it was first thought of like BS and done nothing about. And to Symantech and F-secure who likes to give speeches, try to get your facts right the next time. We don't want you to embarasse yourself, you will surely use this to sell more of your product I trust. And while I have your attention anyway, F-secure, I still have your domain and been waiting for your information where to transfer it…

This is all for now, busy days cleaning out the apartment for anything that could look to be used by terrorists (good thing I don't have any flight simulation games!). We all know how law

(doesn't) works in the US…

"America is the only country that went from barbarism to decadence without civilization in between."

//D

DEranged gives you 100 passwords to Governments & Embassies

August 30th, 2007 by admin | Posted in DEranged Security | 20 Comments »

Here is a list with working passwords to exactly 100 email-accounts to Embassies and Governments around the world. Yes it's the real deal and still working when we are posting this. So why in the world would anyone publish this kind of information? Because seriously, I'm not going to call the president of Iran and tell him that I got access to all their embassies. I'm DEranged, not suicidal! He has bombs and stuff…

Experience tells me that even if I would contact everyone on this list most are not going to listen or perhaps just blame me for being an evil hacker and that no one else would ever find this out. WTF does it take for people to learn!?

Can't throw it away, it's only a matter of time until someone else gets the same information. Or wait, does someone else have this already? For how long have they had it? What are they doing with it?

Selling it would probably make me a fair amount of money but that ain't my style and I'm sure people have disappeared for less.

After trying every scenario in my head I end up dead, in jail or worse.

So fuck it! Here is everything you need to read classified email and fuck up some serious International business. Hopefully this will put light on the security problems that are never talked about and get at least this fixed with a speed that you never seen your government work before. As a Swedish citizen I can't give this information to anyone without getting into trouble, so instead I'm giving it to everyone.

I would like to remind everyone that using ANY of this is a serious crime and I trust that nothing here will be used, ever! If you do anyway you are a fucker, idiot, moron, lamer, scriptkiddie, criminal and obviously don't get the point of this publishing. Private and company accounts gathered are NOT published, we will NEVER put a threat on your company or personal life!

The thousands of classified mail we have read however are for our own pleasure only so MUST or any such organizations don't even bother, they are GONE! Any raid of my place will only find you loads of beer and prove that you don't get the point of DEranged. Swedish cops need more resources and not more job.

Now let's see how many angry mails I will get before I get my free vacation to Guantanamo Bay paid by Mr. Bush.

//D

Who | IP to pop3 | Login | Password

Indian Embassy in Sweden 81.228.8.31 u81004859 Brdv8H5j
Russian Embassy in Sweden 81.228.11.36 u86119749 y9z8ApZp
Kazakhstan Embassy in Russia 81.176.67.157 akmaral@kazembassy.ru 86rb43
Kazakhstan Embassy in Russia 81.176.67.157 alla@kazembassy.ru vhs35
Kazakhstan Embassy in Russia 81.176.67.157 askarest@kazembassy.ru dol57
Kazakhstan Embassy in Russia 81.176.67.157 b.kuatbekova@kazembassy.ru bk145
Kazakhstan Embassy in Russia 81.176.67.157 baimenche@kazembassy.ru 1956
Kazakhstan Embassy in Russia 81.176.67.157 den@kazembassy.ru bek70
Kazakhstan Embassy in Russia 81.176.67.157 emo@kazembassy.ru art35
Kazakhstan Embassy in Russia 81.176.67.157 galikhin@kazembassy.ru aGC4jyf
The Office of Dalai Lama 65.19.137.2 tlc@dalailama.com tsephell
The Office of Dalai Lama 65.19.137.2 tntaklha@dalailama.com dudul5425
The Office of Dalai Lama 65.19.137.2 chhimerigzing@dalailama.com ylypp610
Indian Embassy in Oman 65.109.245.38 da da01877y
Uzbekistan Consulate in France 57.66.151.179 Parij_C p2a2r0i9j
Uzbekistan Consulate in Germany 57.66.151.179 Berlin_C b5a6h7o8r9
Uzbekistan Consulate in India 57.66.151.179 Dehli_C i1n9d5u6
Uzbekistan Consulate in New York 57.66.151.179 Nyu_York_UN t2r7d31ln8
Uzbekistan Consulate in South Korea 57.66.151.179 Seul_C s1e7u0l7c
Uzbekistan Consulate in USA 57.66.151.179 Vashington_c s7a9s5h3a1
Uzbekistan Embassy in Afghanistan 57.66.151.179 AfghanQ a1f2g3h4a5n6q
Uzbekistan Embassy in Afghanistan 57.66.151.179 afghanm a1f1g0h1a0n2m
Uzbekistan Embassy in Belgium 57.66.151.179 Bryussel b1r3y0u2s1
Uzbekistan Embassy in China 57.66.151.179 Pekin e1q8b3n7a2
Uzbekistan Embassy in Dubai 57.66.151.179 dubay b2r7s1d3y4
Uzbekistan Embassy in France 57.66.151.179 Parij u3t1k9i6r2
Uzbekistan Embassy in Germany 57.66.151.179 Frankfurt a8h7f6y5r4
Uzbekistan Embassy in Indonesia 57.66.151.179 jakarta t2d7j3a4m9
Uzbekistan Embassy in Israel 57.66.151.179 Tel_Aviv m1u9z5r6ob
Uzbekistan Embassy in Japan 57.66.151.179 Tokio h5o6n7d8a9
Uzbekistan Embassy in Kuwait 57.66.151.179 kuwait k3u0w0a1i0t6
Uzbekistan Embassy in Kyrgyzstan 57.66.151.179 bishkek a1h4e0y2p1
Uzbekistan Embassy in Latvia 57.66.151.179 Riga z8e2t7w1×5
Uzbekistan Embassy in Malaysia 57.66.151.179 Malayziya g6h8w0e2d3
Uzbekistan Embassy in Pakistan 57.66.151.179 Islomobod y7j2l3b8h1
Uzbekistan Embassy in Poland 57.66.151.179 varshava p0o4l1s1h0a3
Uzbekistan Embassy in Russia 57.66.151.179 Moskva z1a8f0a2r1
Uzbekistan Embassy in Saudi Arabia 57.66.151.179 Jidda j3i1d7d9a5
Uzbekistan Embassy in South Korea 57.66.151.179 seul z1y9×2e0le
Uzbekistan Embassy in Thailand 57.66.151.179 Bangkok n7o8d2i0r5
Uzbekistan Embassy in The Netherlands 57.66.151.179 Amsterdam h1o5l0a2n1
Uzbekistan Embassy in Turkey 57.66.151.179 Anqara g5s2b7×1o4
Uzbekistan Embassy in Turkey 57.66.151.179 Istanbul b5c2n3f4v1
Uzbekistan Embassy in Turkmenistan 57.66.151.179 Ashxobod d7o1m5l6a2
Uzbekistan Embassy in Ukraine 57.66.151.179 Kiev s5c4h3u2h1
Uzbekistan Embassy in United Kingdom 57.66.151.179 London w9r3y7g4d1
Uzbekistan Embassy in United Kingdom 57.66.151.179 London_Elchi l9o8n7d6n5
Uzbekistan Embassy in USA 57.66.151.179 vashington_m e1r2k3i4n5
Uzbekistan Embassy in Uzbekistan 57.66.151.179 toshkent epyan2006
Uzbekistan Embassy in Uzbekistan 57.66.151.179 Toshkent_M 3456789
Uzbekistan Foreign Affairs 57.66.151.179 Qohira 5gx7n1e4w9
Iran Embassy in Ghana 217.172.99.19 iranemb_accra@mfa.gov.ir accra
Iran Embassy in Kenya 217.172.99.19 iranemb_kenya@mfa.gov.ir kenya
Iran Embassy in Oman 217.172.99.19 iranemb_muscat@mfa.gov.ir muscat
Iran Embassy in Tunisia 217.172.99.19 iranemb_tunisia@mfa.gov.ir tunisia

Iran Ministry of Foreign Affairs 217.172.99.19 bagheripour@mfa.gov.ir amir1368
Kazakhstan Embassy in Italy 213.21.159.23 kazakstan.emb@agora.it rfywkth
Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb piramid
Kyrgyztan Embassy in Iran 212.42.96.15 embiran asdfgh
Kyrgyztan Embassy in kazakhstan 212.42.96.15 kaz_emb W34#eEDd
Indian Embassy in Italy 212.34.224.157 m0006614 srpq86m
Indian Embassy in Belgium 212.100.160.114 commercial@indembassy.be india01
Mongolian Embassy in USA 209.213.221.249 esyam@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 j.mendee@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 n.tumenbayar@mongolianembassy.us temp
UK Visa Application Centre in Nepal 208.109.119.54 vfsuknepal@vfs-uk-np.com Password
Kazakhstan Embassy in Japan 203.216.5.113 embkazjp nf5!3LeG
India National Defence Academy 203.199.162.245 mis misadmin
Hong Kong Human Rights Monitor 203.161.254.182 po@hkhrm.org.hk T5a*4V#K
Hong Kong Legislative Council member 203.124.10.110 billywong@mandytam.com 232880
Hong Kong Legislative Council member 203.124.10.110 tim@mandytam.com 220866
Hong Kong Legislative Council member 202.66.159.18 poppy@ronnytong.org rtppy346
One Country Two Systems Research Institute of China 202.66.107.12 kenchan@octs.org.hk 153kenchan
Liaison Office of the Dalai Lama for Japan & East-Asia 202.208.210.8 tibet02 TIBET310
Hong Kong Legislative Council member 202.181.132.82 margaret@margaretng.com sarah#
Hong Kong Legislative Council member 202.181.132.68 hazelpun@sinchungkai.org.hk 9cxh6gpy
Hong Kong Legislative Council member 202.181.132.68 chungkai@sinchungkai.org.hk Yvonne0328
Hong Kong Democratic Party 202.177.28.170 twk@dphk.org password
Hong Kong Liberal Party 202.123.79.164 miriamlau 123456
Hong Kong Liberal Party 202.123.79.164 tinyan 12345678
Hong Kong Liberal Party 202.123.79.164 pauline 25334264
Hong Kong Liberal Party 202.123.79.164 wilkin x105×10a
Hong Kong Liberal Party 202.123.79.164 joy 26606624
Hong Kong Association for Democracy & People's Livelihood Party 202.123.216.231 hmt@adpl.org.hk hmt27622676
Hong Kong Association for Democracy & People's Livelihood Party 202.123.216.231 info@adpl.org.hk info27823137
Hong Kong Association for Democracy & People's Livelihood Party 202.123.216.231 iggyng@adpl.org.hk igg27823137
Hong Kong Association for Democracy & People's Livelihood Party 202.123.216.231 fcc@adpl.org.hk fcc22674595
Indian Embassy in China 202.109.110.87 amb@indianembassy.org.cn 1234
Indian Embassy in China 202.109.110.87 amboff@indianembassy.org.cn 1234
Tajikistan Embassy in China 202.106.46.87 tjkemb w4u7e3a2
Indian Embassy in Germany 194.95.249.247 rb1002p1 consind1
Indian Embassy in Germany 194.95.249.247 rb1002p15 com15ind
Kazakhstan Consulate General in China 194.67.23.102 kzconsulshanghai 987654
Japan Embassy in ? 194.226.128.37 emb_japan_ast4 123456
Indian Embassy in Finland 193.229.0.46 kv7198 npyrhdjj
Hong Kong Goverment Information Service Department Goverment 147.8.219.202 erika.chau 60777699
China Civil Human Right Front 123.242.224.80 contact@civilhrfront.org 17891894
China Civil Human Right Front 123.242.224.80 secretariat@civilhrfront.org 17891894
Defence Research & Development Organisation Govt. Of India, Ministry of Defence jpsingh@drdo.com password+1
Indian Embassy in USA amb@indianembassy.org 1234
Sorry for the bad layout, we will have to fix that =)

DEranged Security

- Search

- ## Pages
  - About
- ## Archives
  - September 2007
  - August 2007
- ## Categories
  - DEranged Security (4)

Powered by WordPress
Designed by Bob
Top