

RFX NETWORKS ALERT

Source: <http://linux.derkeiler.com/Newsgroups/alt.linux/2004-02/0326.html>

From: Ryan (ryan_at_rfxnetworks.com)

Date: 02/10/04

Date: Tue, 10 Feb 2004 06:02:03 GMT

Some of you might have been affected by this. My website was hacked and the below was posted to some security websites. If I did security for any of you, please check below and see if any of the root login/password for your servers were made public by the hackers. Sorry

Extra! Extra! Read all about it!

What's the word of the day? Who's the word of the day? Wake up to sunny skies or a stormy mornin?

What have we got for you today? We've got another kid from the security realm trying to profit from the exploitations of others... one with no warrant or education to be charging for his services.

Who could this be you may ask... who, that knows didly shit, is trying to make money in the security industry?

The answer: Way too fucking many people... damn straight.

So, lets begin fucking each of them over... and over... and over until they are as reputable as your neighborhood two-buck whore.

Name: Ryan MacDonald

Company: RFXNetworks ryan@r-fx.org/ryan@rfxnetworks.com

| R-fx Networks offers industry leading managed services
| that are priced below that of many competitors. No setup
| fees or hidden costs with any service, and all services
| backed by a 30 day money back guarantee.
|

| We are specialized consultants with years of experience
| in Linux, BSD, Windows, and Solaris. Our knowledge resides
| in security and scalable server management on varying levels.
| Not only do we provide services at below-market rates but we

| also innovate.

| Our services are often complimented in one fashion or
| another by software we have developed on our own, such (free)
| software includes:

| Advanced Policy Firewall (APF) – <http://www.r-fx.net/apf.php>
| System Integrity Monitor (SIM) – <http://www.r-fx.net/sim.php>
| System Backup (SysBK) – <http://www.r-fx.net/sysbk.php>

| We also make available exclusive software to clients, and as
| well we customize or develop to client needs any software
| to suite the task at hand. So trust your valued assets in the
| hands of experienced innovators with the solid and proven
| services provided by r-fx.net.

| An introductory level monitoring & management solution. This
| provides basic emergency response and remote availability
| monitoring. Likewise it is also complimented by a local system
| monitor to take action during situations of service failure (SIM).

| Summary of features:

- | – SIM (System integrity monitor)
- | – Remote services and availability monitor; pager/sms/email alerts
- | – Emergency 24/7 support; pager contact (8 hours per/mo)

| Starting at \$30/mo; Discount
| rates apply for 3 or more servers (8% discount per/server).

| An intermediate monitoring & management solution. This provides
| advanced support services, emergency support and on-demand software
| installations. It is the focus of this package to maintain integrity,
| this is done via a scaled security bundle setup and custom installed
| applications.

| Summary of features:

- | – Custom firewall setup; APF (Advanced policy firewall) [optional]
- | – SIM (System integrity monitor)
- | – PRM (Process resource monitor)
- | – FaF (File anomaly finder)
- | – PMON (Network socket monitor)
- | – SPRI (System priority)
- | – Remote services and availability monitor; pager/sms/email alerts
- | – Auto-update service for RPM-based software (hourly repository check-up)
- | – Basic trouble shooting support (10 hours per/mo)
- | – Emergency 24/7 support; pager contact (10 hours per/mo)
- | – Free one-time scaled setup of security bundle
- | – Request based software setup (4 hours per/mo) Avg. software install time
15 minutes

alt.linux: RFX NETWORKS ALERT

– Hardware, resources and future scalability assessment (upon request)
|
| Starting at \$85/mo; click here for more information. Discount rates
| apply for 3 or more servers (15% discount per/server).
|
| Visit R–fx Networks; Managed Services home page today for this and other
great deals.
| Private consulting starts at \$30/hr and is negotiable; custom solutions
available upon request.

He almost makes people think he knows what he is doing, and that he deserves
money
for his time. We have determined that Mr. Ryan MacDonald of RFXNetworks has
not only
defrauded his customers, but also exploited their lack of intelligence
through over–charging
for his services, while also leaving the integrity of his client's servers
open to the
whole world. To demonstrate this lack of care, integrity, and intelligence
by Mr. Ryan MacDonald
we will display the information for a number of his clientele. All below
server information
is valid as of 3pm Eastern Time Zone February 3, 2004. Got Root?

~e18

1) Server hostname/IP
cpanel.servdns.net / 69.56.220.66

2) Server login information
root
ddexbyfartknocker

Your Domain Name is: globalville.com
Your IP Address is: 216.40.227.218
Your Gateway is: 216.40.227.1
Your Server login ID is: admin
The admin password is: ClXhA9sJ2uC

1) Server hostname/IP --> 69.56.205.66
2) Server login information --> root/Minetar0

IP: 69.57.148.21

user: root
Password: jjEPsTabj27

RFX NETWORKS ALERT

alt.linux: RFX NETWORKS ALERT

server hostname: ns3.potia.net
server ip :64.62.172.20
login : username: hellouk passsword:my0817potia
su – password: king0817lear

My Base IP Address is: 207.36.180.50

For all applications on my server:

the Username= admin / root
Password= zrx154451

Ensim Login Information:

<http://207.36.180.50/admin/>

Server1:
srv1.noc-servers.com/66.246.37.12 located at dedicated now. RH 7.3 root
7428pbv

Server2:
mercury.noc-servers.com/64.191.51.125 located at nocster.com RH 7.3 root
7428pbv

Server3:
zinc.noc-servers.com/216.67.228.232 located at Dedicatednow RH 7.3 root
7428pbv

Server4:
copper.noc-servers.com/64.5.48.42 located at The Planet. RH 8.0 root 7428pbv

Server5:
silver.noc-servers.com/64.5.51.44 located at The Planet RH 7.3 root 7428pbv

Server6:
bronze.noc-servers.com/69.56.188.210 located at The Planet RH 9.0 root
7428pbv

66.79.165.150
username: root
password: cial124x

My server ip is: 66.79.162.40

Additional ip's are: 66.79.162.40 — 66.79.162.49

Access via SSH

alt.linux: RFX NETWORKS ALERT

u: root
p: jac1124x

Server hostname/IP:
alpha.verkkomestari.com / 66.246.110.187

Server login information:
root / cleZOas4

Server = P4 2.4Ghz 1.5GB Ram (Dell PowerEdge)

root pass = iloveryan

64.246.62.21

ADMIN: XO1m16j-3_
root: S1h#2)Kc7U

1. moi.herem8.com 207.44.244.93

2. admin tur69ip
root V%4rN#8n

IP: 69.57.148.21
admin user: root
password: 9ep27WsT

This is a Red Hat Linux 9 server.

Hostname: cb.fxsonet.com
Password: orange777

einstein.datadork.com
207.44.214.64

login: root
password: 78737dork

ip: 64.246.32.71
root
yadiczwnx

1) Server hostname/IP
chubby.nameserve.org / 64.62.138.166

2) Server login information
root / 420dv2getfucked

- The server hostname is july.dnsanonymous.com with the IP being

alt.linux: RFX NETWORKS ALERT

209.50.233.248

2 – Direct root access is currently disabled for the server. You can login by connecting to the IP 209.50.233.248 on port 8888 using SSH. The login name is dnsanon and the password is liber mortus. You will then be able to su into root using the password 94slIm6choC10

HOST: www.xiteworks.net
IP: 216.127.74.25
Login: admin / rcl20c

zeus.selectservers.net / 207.44.244.40

Root PW:

":X0zzSQs/Mk+ii%>haJ0(DJv3"M?B(qEMKb|Vv>]q'ZU

cz.fxsonet.com – 209.123.13.137. It's a Qsol P1.8ghz 512mb RAM RH Linux 7.3 machine. It's a live machine with over 300 websites on.

It's run cPanel too. There is APF and SIM installed although they are old versions. It's root password is morningglory

IP: 216.127.82.86
user: root
pass: SENECAemma06

66.227.5.25 (ns1.sevaa.com)
root:bxXp9pfE – Ensime: u: 20228 / p: qL5t737r

Server hostname/IP
server3.dc43.com / 216.180.242.122
root/r3@DB00k

207.44.210.52
admin lk7y3gs6
root 8lok3gr

IP address: 66.154.60.30
Root password: 3KA15DWT
other servers are:
STORM
COBRA
TYPHOON
HORNET
FALCON
HAWK
EAGLE
PHANTOM
RAPTOR
TIGER

RFX NETWORKS ALERT

alt.linux: RFX NETWORKS ALERT

RALLY
GALAXY
MERCURY
MUSTANG
SPIRIT
VIKING
PANTHER
BLITZ

You should be able to add .unitedhosting.co.uk to the end of any of those to get its hostname.

login admin/657317

to goto root the pass format is hAn657servername
(replace server name with the servername, not caps).

64.246.60.45

login info is: username: 'admin' password: '11b1do'

server1.dc43.com / 69.56.133.130

2)

root / d3l4m41n

My new server ip is: 69.57.140.72

the admin password is: hawkeyepierce

the root password is: denmark

If Ryan McDonald of RFXNetworks cannot secure his own systems, and as such the root information of your servers which you paid for him to secure are public to the world... would it make you happy?