

## RBN - 365fastcash, Panama, and 1488 RU

As regular readers know the Russian Business Network (RBN) originally utilized an extensive virtual base in Panama (Nevacon), we can now report they are back. The new hive centers on AS26426 Optynex Telecom Sa, Calle 53, Piso 18, Panama City, Panama) Phone: 210-9900 and cybercastco.com name servers (special thanks to Jim McQuaid and Snort expertise).

There are numerous domains but to select a sample of domains, in this article we can focus on two, 365fastcash(dot)com and Jidov(dot)net. It is also pleasing to show these are already encompassed within RBN Snort Rules on EmergingThreats.net (bleeding-rbn-BLOCK.rules)

365fastcash has been delivering a truly blended threat by using an automated telephone dialing system to ask people for the last 4 digits of their social security number. This was flooding switchboards at a well known US charitable organization a few days ago, and was obviously the first of many.

Interestingly there are two sub-domains "back1.365fastcash" and "bavk1.365fastcash" both are similar structures to earlier reported 76service and 76team. The difference on this occasion the likely personal ID data storage is on direct links from the sub-domains to Level3 Communications; box(dot)net, a service that provides the ability to collaborate and share files online. No doubt Level 3 will be able to inform US authorities of the content of these data files, and terminate such services. Further IP and SSL details below.

Jidov(dot)net provides an interesting political twist for the RBN as this is the safe hosting location for 1488(dot)ru. To those who are not aware 1488 RU is the supposedly banned, violent, and very well financed Russian Nazi group. The 14 represents the 14-word slogan: "We must secure the existence of our people and a future for White children" and 88 represents eighth letter of the alphabet, with HH standing for Heil Hitler. The question now arises does this represent the source of the RBN's political views or just an expensive bullet proof (was) hosting.

Forum Intro:

(RU) @C7LO, <K @04K A>>1I8BL 0<, GB> B5?5@L A09B 1488.ru 4>ABC?5= 87 4><5===>9 7>=K Jidov.net . 0728B85 ?>5:B0 845B ?>;=K< E>4><. ;03>40@8< 0A 70 2=8<0=85 : =0H5<C @5AC@AC. !:>@> <K A<>65< ?@54;>68BL 0< @538AB@0F8N 4><5=>2 B@5BL53> C@>2=O 2 =0H8E 4><5==KE 7>=0E ( 0H =8:.1488.ru 8 0H =8:.jidov.net). "0: 65, <K 3>B>2K ?@54;>68BL 20< @07<5I5=85 10=5@>2 =0 AB@0=8F0E =0H53> @5AC@A0.

(EN) Friends, we are glad to report to you that now the site to 1488.ru is accessible from the domain zone Jidov.net. The development of design occurs full speed. We thank you for the attention to our resource. Soon we will be able to propose to you registration it is pre-barter the third level in our domain zones (your nik.1488..ru and your it nik..jidov.net). So, we are prepared to propose to you the arrangement of banners for the pages of our resource.

Further details: 365Fastcash - 200.115.173.215 - Registrar: KEY-SYSTEMS GMBH, Whois Server: whois.rrp-proxy.net  
Name Server: NS1.CYBERCASTCO.COM, NS2.CYBERCASTCO.COM: 06-dec-2007

#### SSL Information for 200.115.173.215

##### SSLv2

Yes

Cipher Spec: SSL2\_RC4\_128\_WITH\_MD5 [010080]

Cipher Spec: SSL2\_RC2\_CBC\_128\_CBC\_WITH\_MD5 [030080]

Cipher Spec: SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5 [0700c0]

Cipher Spec: SSL2\_DES\_64\_CBC\_WITH\_MD5 [060040]

Cipher Spec: SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5 [020080]

Cipher Spec: SSL2\_RC2\_CBC\_128\_CBC\_WITH\_MD5 [040080]

Connection ID: 26ad291530a4cc910e9c066877bda0f0

##### SSLv3

Yes

Cipher Spec: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (256 bit) [000039]

##### TLS 1.0

Yes

Cipher Spec: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (256 bit) [000039]

JIDOV(dot)NET - 200.115.171.200 Registrar: ESTDOMAINS; Name Servers: NS1.CYBERCASTCO.COM, NS2.CYBERCASTCO.COM, 11-nov-2007

SSL Information for 200.115.171.200

SSLv2

Yes

Cipher Spec: SSL2\_RC4\_128\_WITH\_MD5 [010080]

Cipher Spec: SSL2\_RC2\_CBC\_128\_CBC\_WITH\_MD5 [030080]

Cipher Spec: SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5 [0700c0]

Cipher Spec: SSL2\_DES\_64\_CBC\_WITH\_MD5 [060040]

Cipher Spec: SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5 [020080]

Cipher Spec: SSL2\_RC2\_CBC\_128\_CBC\_WITH\_MD5 [040080]

Connection ID: 26ad291530a4cc910e9c066877bda0f0

SSLv3

Yes

Cipher Spec: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (256 bit) [000039]

TLS 1.0

Yes

Cipher Spec: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (256 bit) [000039]