

NATIONAL
INFRASTRUCTURE
PROTECTION
CENTER

August 10, 1998

MEMORANDUM

From: ██████████ NCIS
TO: CIU Chief
SSA ██████████

Subj: WRIGHT PATTERSON AIR FORCE BASE
VICTIM; CITA - COMPUTER INTRUSION
288-CI-NEW

1. As requested by ██████████ I forwarded a request to the Fleet Intelligence Warfare Center (FIWC) to provide all information relating to the following Russian ISPs:

Cityline.ru
Microdin.ru
Sovam.com
Orc.ru
Demos.net
Demos.su

b6
b7c

Additionally, the following passwords and tools/usernames were researched:

Passwords:

██████████
██████████

Tools/usernames:

██████████
██████████
██████████

2. Attached are the results of a search of FIWC's database. The FIWC will report any additional information pertinent to this tasking as it becomes available.

██████████

cityline.ru
Name: ns1.cityline.ru
Address: [REDACTED]

inetnum: [REDACTED]
netname: CITYLINERU
descr: Cityline offers dial-up and leased line access to Internet
descr: for Moscow and St.Peterburg regions.
country: RU
admin-c: AD705-RIPE
tech-c: MB427-RIPE
status: ASSIGNED PA
notify: Error! Bookmark not defined.
mnt-by: CITYLINERU-MNT
source: RIPE

b7E

route: [REDACTED]
descr: Cityline offers dial-up and leased line access to Internet
descr: for Moscow and St.Peterburg regions.
origin: AS8498
notify: Error! Bookmark not defined.
mnt-by: CITYLINERU-MNT
source: RIPE

b6

person: [REDACTED]
address: Cityline
address: [REDACTED]
address: [REDACTED]
phone: [REDACTED]
fax-no: +7 095 245 8877
e-mail: Error! Bookmark not defined.
nic-hdl: AD705-RIPE
notify: Error! Bookmark not defined.
source: RIPE

b7C

person: [REDACTED]
address: [REDACTED]
address: [REDACTED]
address: [REDACTED]
phone: [REDACTED]
e-mail: Error! Bookmark not defined.
nic-hdl: MB427-RIPE
source: RIPE

(Handwritten mark)

microdin.ru (NAVCIRT Incident 98-5 of 6Jan98)

Name: microdin.ru

Address: [REDACTED]

inetnum: [REDACTED]

netname: MICRONET

descr: MicroNet Ltd.

descr: Requested network ip numbers will be used for connecting

descr: to MAcomnet.

country: RU

admin-c: SB1164-RIPE

tech-c: DV86-RIPE

status: ASSIGNED PA

notify: Error! Bookmark not defined.

source: RIPE

b7E

route: [REDACTED]

descr: Micronet Ltd.

descr: 18 Novozavodskaya st

descr: Moscow Russia 121309

origin: AS8470

notify: Error! Bookmark not defined.

notify: Error! Bookmark not defined.

mnt-by: MACOMNET-MNT

source: RIPE

b6
b7C

person: [REDACTED]

address: MicroNet Ltd.

address: 18, Novozavodskaya st

address: 121309, Moscow, Russia

phone: +7 095 145-9520

phone: +7 095 145-9522

phone: +7 095 142-0618

fax-no: +7 095 924-0464

e-mail: Error! Bookmark not defined.

nic-hdl: SB1164-RIPE

source: RIPE

person: [REDACTED]

address: [REDACTED]

address: [REDACTED]

address: [REDACTED]

phone: [REDACTED]

e-mail: Error! Bookmark not defined.

nic-hdl: DV86-RIPE

source: RIPE

(2)

sovam.com
 sovam.com preference = 200, mail exchanger = relay2.sovam.com
 sovam.com preference = 100, mail exchanger = relay1.sovam.com
 sovam.com nameserver = ns2.sovam.com
 sovam.com nameserver = nic.near.net
 sovam.com nameserver = pandora.sf.ca.us
 sovam.com nameserver = ns.sovam.com
 relay2.sovam.com internet address = [REDACTED]
 relay1.sovam.com internet address = [REDACTED]
 ns2.sovam.com internet address = [REDACTED]
 nic.near.net internet address = [REDACTED]
 pandora.sf.ca.us internet address = [REDACTED]
 ns.sovam.com internet address = [REDACTED]
 [rs.internic.net]

b7E

Registrant:
 Sovam Teleport (SOVAM-DOM)
 2A Nezhdanova st
 Moscow, Russia 109003
 RU

Domain Name: SOVAM.COM

Administrative Contact:
 [REDACTED] (KA41) Error! Bookmark not defined.

Technical Contact, Zone Contact:
 Semenyuk, Igor (IS13) Error! Bookmark not defined.

Record last updated on 19-Mar-98.
 Record created on 22-Jan-93.
 Database last updated on 6-Aug-98 04:06:34 EDT.

b6
b7c

Domain servers in listed order:

NS.SOVAM.COM [REDACTED]
 NS2.SOVAM.COM [REDACTED]
 NIC.NEAR.NET [REDACTED]

inetnum: [REDACTED]
 netname: [REDACTED]
 descr: Sovam Teleport
 descr: Moscow, Russia
 country: RU
 admin-c: AK57-RIPE
 tech-c: IS13
 rev-srv: ns.sovam.com
 rev-srv: ns2.sovam.com
 rev-srv: nic.near.net

(2)

status: ASSIGNED PA
notify: Error! Bookmark not defined.
mnt-by: AS3216-MNT
source: RIPE

route: [REDACTED]
descr: SOVAM DELEGATED BLOCK-1
origin: AS3216
advisory: AS690 1:3561 2:1128
notify: Error! Bookmark not defined.
mnt-by: AS3216-MNT
source: RIPE

b7E

person: [REDACTED]
address: SOVAM TELEPORT Company Ltd.
address: [REDACTED]
address: [REDACTED]
address: [REDACTED]
phone: [REDACTED]
fax-no: +7 095 2584133
e-mail: Error! Bookmark not defined.
nic-hdl: AK57-RIPE
source: RIPE

b6

b7C

person: [REDACTED]
address: SOVAM TELEPORT Company Ltd.
address: [REDACTED]
address: [REDACTED]
address: [REDACTED]
phone: [REDACTED]
phone: [REDACTED]
fax-no: +7 095 2584133
e-mail: Error! Bookmark not defined.
nic-hdl: IS13
source: RIPE

(4)

orc.ru
 orc.ru preference = 20, mail exchanger = mail2.ras.ru
 orc.ru preference = 5, mail exchanger = mail.orc.ru
 orc.ru preference = 10, mail exchanger = mail1.orc.ru
 orc.ru preference = 15, mail exchanger = mail1.ras.ru
 orc.ru nameserver = ns.orc.ru
 orc.ru nameserver = nss.orc.ru
 orc.ru nameserver = nss.msu.ru
 mail2.ras.ru internet address = [REDACTED]
 mail1.orc.ru internet address = [REDACTED]
 ns.orc.ru internet address = [REDACTED]
 nss.orc.ru internet address = [REDACTED]
 nss.msu.ru internet address = [REDACTED]

b6
 b7c

[rs.internic.net]
 [No name] (NS31095-HST)

[REDACTED]

Hostname: NS.ORG.RU
 Address: [REDACTED]
 System: ? running ?

Coordinator:

[REDACTED] CAH30) Error! Bookmark not defined.

Record last updated on 18-Sep-97.
 Database last updated on 6-Aug-98 04:06:34 EDT.

demos.net (Navcirt 98-6211 of 3 Aug 98)
 demos.net preference = 50, mail exchanger = relay1.demos.su
 demos.net preference = 100, mail exchanger = relay2.demos.su
 demos.net nameserver = ns.demos.su
 demos.net nameserver = ns1.demos.net
 relay1.demos.su internet address = [REDACTED]
 relay2.demos.su internet address = [REDACTED]
 ns.demos.su internet address = [REDACTED]
 ns.demos.su internet address = [REDACTED]
 ns1.demos.net internet address = [REDACTED]
 [sequoia.ripe.net]

b7c

inetnum: [REDACTED]
 netname: DEMOS-CORP
 descr: DEMOS Corporate Network

(5)

descr: Demos Plus Co. Ltd.
descr: Moscow, Russia
country: RU
admin-c: PA75
tech-c: ED12-RIPE
tech-c: GB90-RIPE
tech-c: GK41-RIPE
mnt-by: AS2578-MNT
source: RIPE

b7E

route: [REDACTED]
descr: DEMOS
origin: AS2578
notify: Error! Bookmark not defined.
mnt-by: AS2578-MNT
source: RIPE

person: [REDACTED]
address: Demos Plus Ltd.
address: Ovchinnikovskaya nab. 6/1
address: Moscow 113035
address: Russia
phone: +7 095 9566233
phone: +7 095 9566234
fax-no: +7 095 9565042
e-mail: Error! Bookmark not defined.
nic-hdl: PA75
source: RIPE

b6
b7c

person: [REDACTED]
address: Demos Company Ltd.
address: 6-1 Ovchinnikovskaya nab.
address: Moscow 113035
address: Russia
phone: +7 095 956 6233
phone: +7 095 956 6234
fax-no: +7 095 233 5016
e-mail: Error! Bookmark not defined.
nic-hdl: ED12-RIPE
notify: Error! Bookmark not defined.
source: RIPE

6

demos.su
 demos.su preference = 100, mail exchanger = relay2.demos.su
 demos.su preference = 50, mail exchanger = relay1.demos.su
 demos.su nameserver = ns.demos.su
 demos.su nameserver = ns1.demos.net
 demos.su nameserver = ns.ussr.eu.net
 relay2.demos.su internet address = [REDACTED]
 relay1.demos.su internet address = [REDACTED]
 ns.demos.su internet address = [REDACTED]
 ns.demos.su internet address = [REDACTED]
 ns1.demos.net internet address = [REDACTED]
 ns.ussr.eu.net internet address = [REDACTED]

b7E

% Rights restricted by copyright. See Error! Bookmark not defined.

inetnum: [REDACTED]
 netname: RU-DEMOS-970415
 descr: PROVIDER
 descr: Demos Company Ltd.
 country: RU
 admin-c: ED12-RIPE
 admin-c: AAP1-RIPE
 tech-c: SL6-RIPE
 tech-c: OB36-RIPE
 status: ALLOCATED PA
 mnt-by: RIPE-NCC-HM-MNT
 source: RIPE

b6

route: [REDACTED]
 descr: DEMOS
 origin: AS2578
 notify: Error! Bookmark not defined.
 mnt-by: AS2578-MNT
 source: RIPE

b7C

person: [REDACTED]
 address: Demos Company Ltd.
 address: 6-1 Ovchinnikovskaya nab.
 address: Moscow 113035
 address: Russia
 phone: +7 095 956 6233
 phone: +7 095 956 6234
 fax-no: +7 095 233 5016
 e-mail: Error! Bookmark not defined.
 nic-hdl: ED12-RIPE
 notify: Error! Bookmark not defined.
 source: RIPE

7

person: [REDACTED]
 address: Russian Institute for Public Networks
 address: 1, Kurchatov sq
 address: Moscow
 address: Russia
 phone: +7 095 1967278
 fax-no: +7 095 1964984
 e-mail: Error! Bookmark not defined.
 nic-hdl: AAPI-RIPE
 remarks: Admin contact for SU domain
 remarks: xSU/RU NIC contact
 source: RIPE

b6
b7c

person: [REDACTED]
 address: Russian Institute for Public Networks
 address: 1 Kurchatov square
 address: 123182 Moscow
 address: Russia
 phone: +7 095 196 7363
 fax-no: +7 095 196 4984
 e-mail: Error! Bookmark not defined.
 nic-hdl: SL6-RIPE
 source: RIPE

person: [REDACTED]
 address: Russian Institute for Public Networks
 address: 1 Kurchatov square
 address: 123182 Moscow
 address: Russia
 phone: +7 095 192 7933
 fax-no: +7 095 946 9841
 e-mail: Error! Bookmark not defined.
 nic-hdl: OB36-RIPE
 notify: Error! Bookmark not defined.
 source: RIPE

8

IP Incident hits:

cityline.ru

[REDACTED]

microdin.ru

[REDACTED]

sovam.com

[REDACTED]

orc.ru

no hits on old database (to mid Jul 1998)

demos.net

[REDACTED]

demos.su

no hits on old database (to mid Jul 1998)

b7E

(9)