RSA CONFERENCE 2013

New Ways of Mitigating Botnets

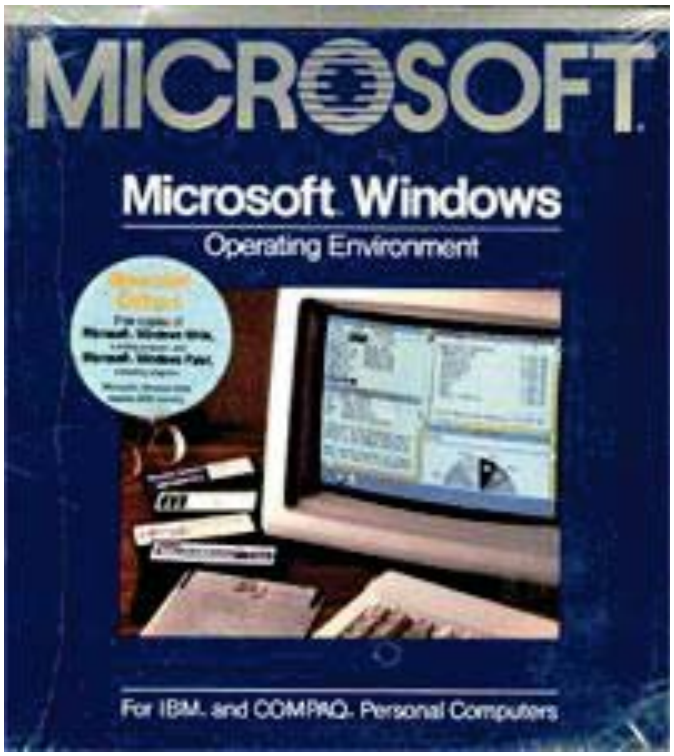
Mikko Hypponen
CRO, F-Secure
@mikko

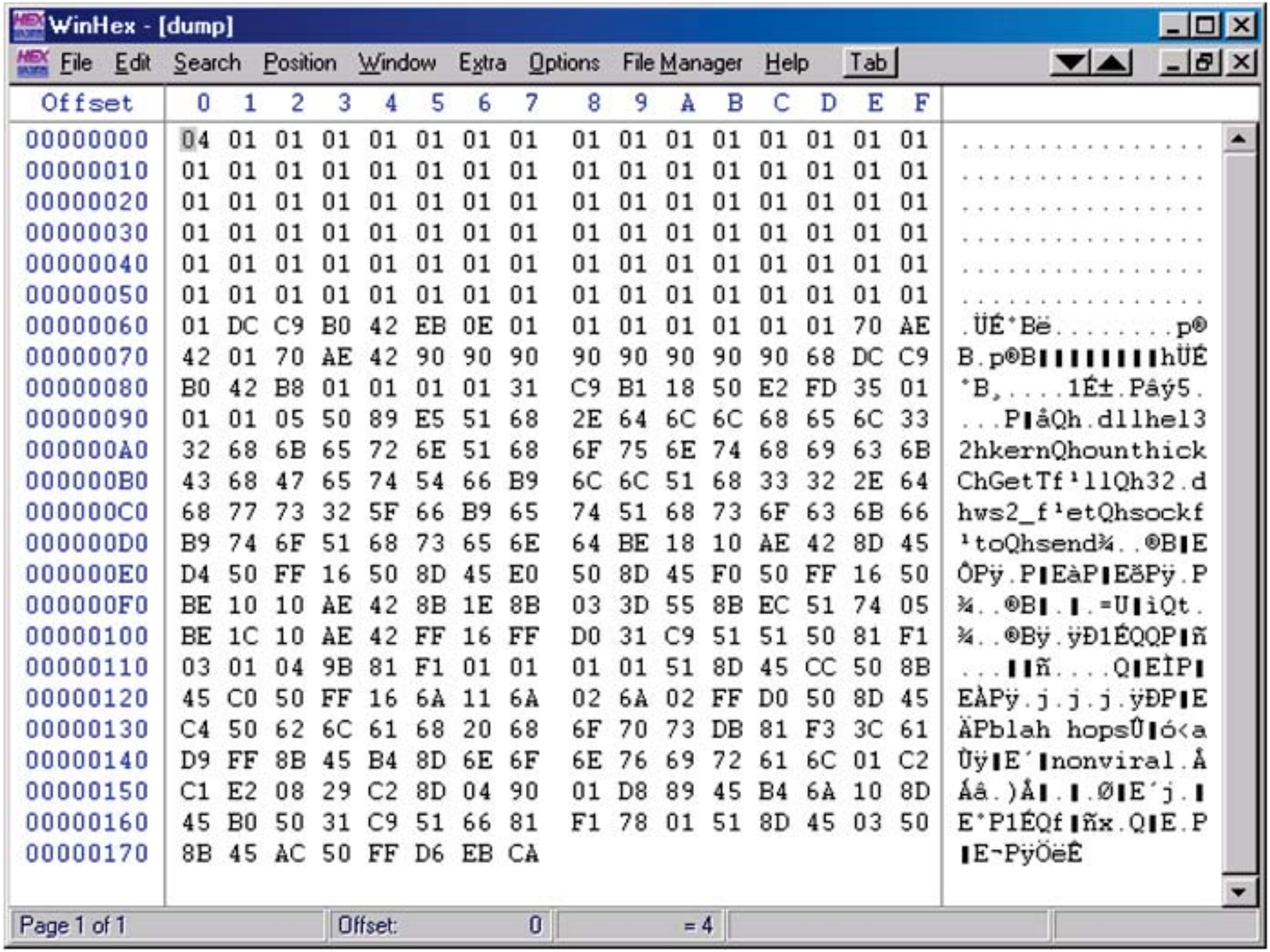
Security in knowledge

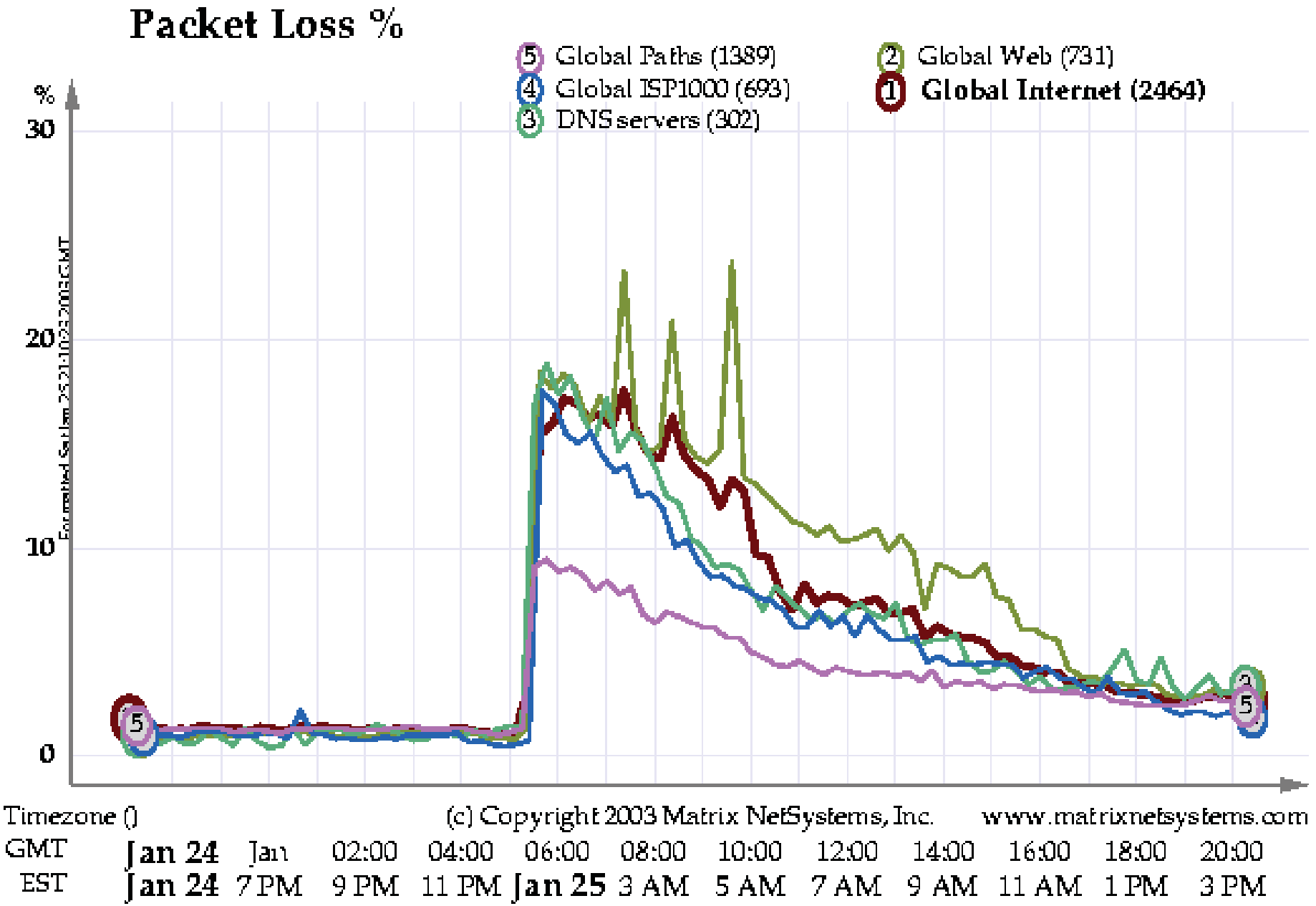
F-Secure

Session ID: BR-R33

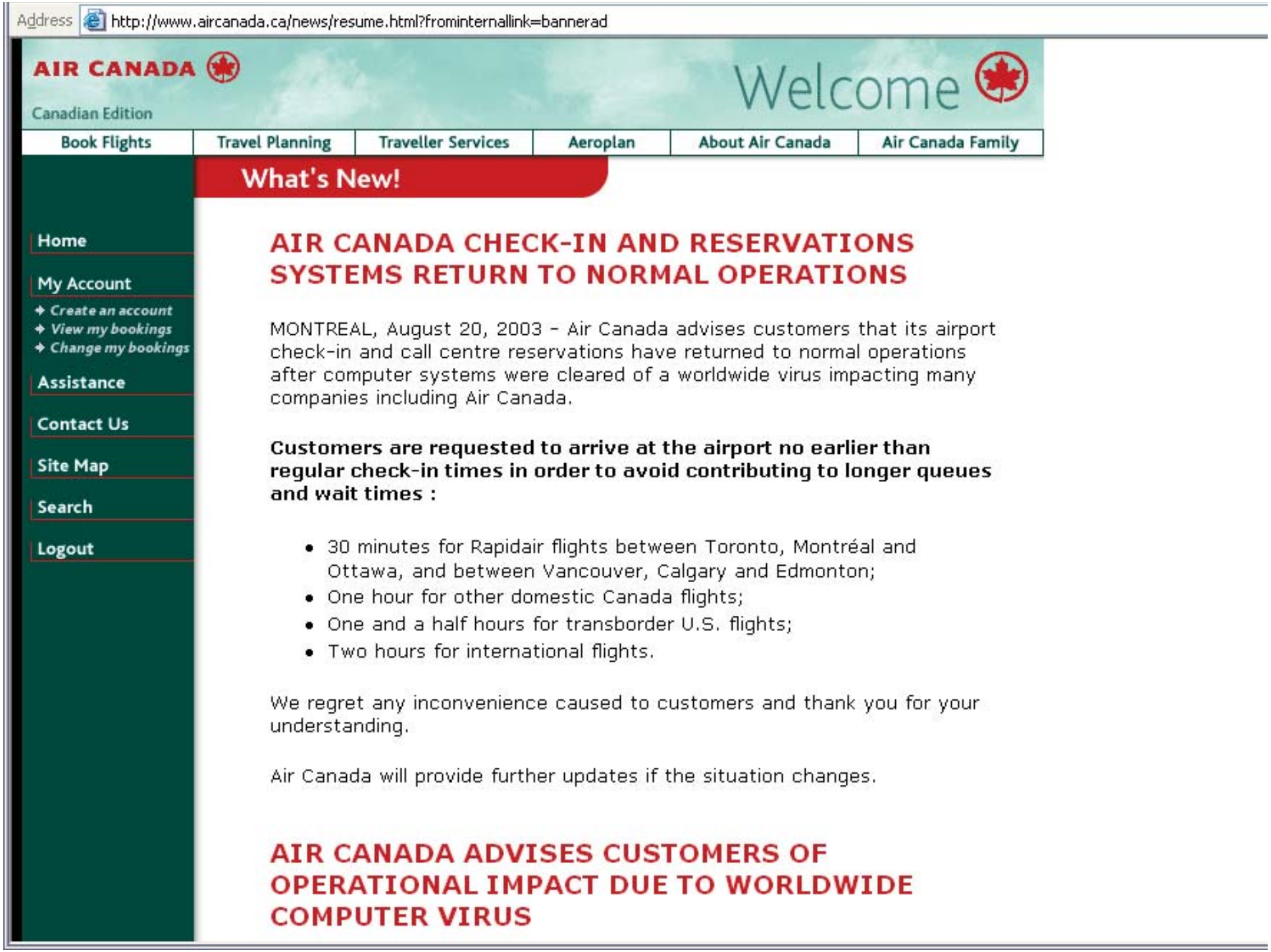
Session Classification: Rated R For Adults Only


MICROSOFT
Microsoft Windows
Operating Environment
For IBM- and COMPAQ- Personal Computers


WinHex - [dump]
File Edit Search Position Window Extra Options File Manager Help Tab
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 04 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000010 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000020 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000030 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000040 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000050 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00000060 01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 01 70 AE
00000070 42 01 70 AE 42 90 90 90 90 90 90 90 90 68 DC C9
00000080 B0 42 B8 01 01 01 01 31 C9 B1 18 50 E2 FD 35 01
00000090 01 01 05 50 89 E5 51 68 2E 64 6C 6C 68 65 6C 33
000000A0 32 68 6B 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B
000000B0 43 68 47 65 74 54 66 B9 6C 6C 51 68 33 32 2E 64
000000C0 68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66
000000D0 B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45
000000E0 D4 50 FF 16 50 8D 45 E0 50 8D 45 F0 50 FF 16 50
000000F0 BE 10 10 AE 42 8B 1E 8B 03 3D 55 8B EC 51 74 05
00000100 BE 1C 10 AE 42 FF 16 FF D0 31 C9 51 51 50 81 F1
00000110 03 01 04 9B 81 F1 01 01 01 01 51 8D 45 CC 50 8B
00000120 45 C0 50 FF 16 6A 11 6A 02 6A 02 FF D0 50 8D 45
00000130 C4 50 62 6C 61 68 20 68 6F 70 73 DB 81 F3 3C 61
00000140 D9 FF 8B 45 B4 8D 6E 6F 6E 76 69 72 61 6C 01 C2
00000150 C1 E2 08 29 C2 8D 04 90 01 D8 89 45 B4 6A 10 8D
00000160 45 B0 50 31 C9 51 66 81 F1 78 01 51 8D 45 03 50
00000170 8B 45 AC 50 FF D6 EB CA
Page 1 of 1
Offset: 0
= 4

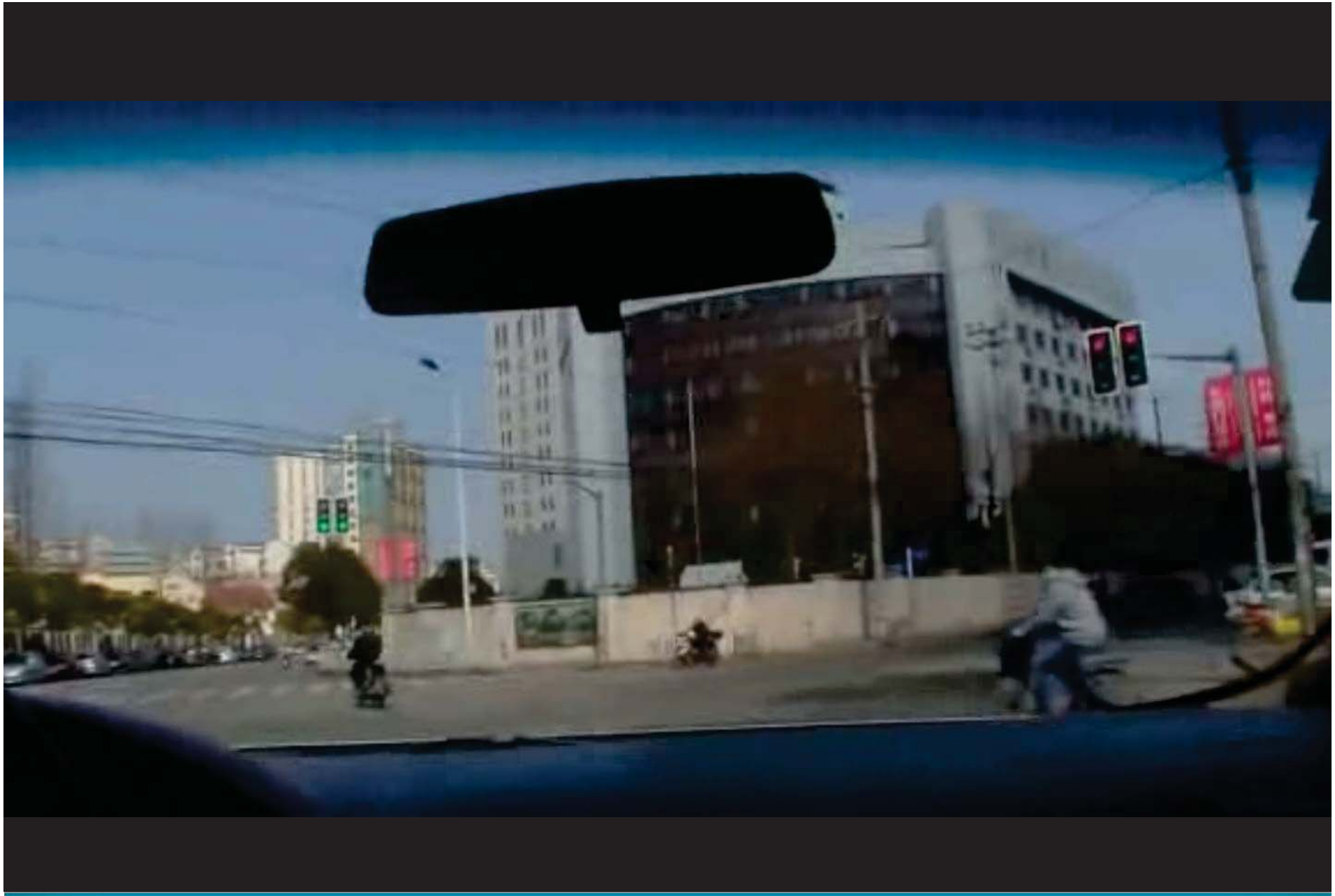

Packet Loss %
5 Global Paths (1389)
4 Global ISP1000 (693)
3 DNS servers (302)
2 Global Web (731)
1 Global Internet (2464)
%
30
20
10
0
Timezone ()
(c) Copyright 2003 Matrix NetSystems, Inc.
www.matrixnetsystems.com
GMT Jan 24 Jan 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00
EST Jan 24 7 PM 9 PM 11 PM Jan 25 3 AM 5 AM 7 AM 9 AM 11 AM 1 PM 3 PM

	Transportation	Power	Infrastructure	Banks
Slammer	Air traffic control problems in USA	Infected a nuclear power plant in Ohio	911 phone services down in Seattle	Bank of America's ATM network down
Blaster	Air Canada flights grounded, CSX trains stopped	NY ISO power operator's network infected	Numerous RPC-based SCADA networks down	Several Windows-based ATM networks infected
Sasser	Railcorp trains stopped in Australia, Delta flight problems, delays with British Airways flights	Hong Kong government's department of energy networks infected	Infected: Two hospitals in Sweden, EU commission, Heathrow airport, Coastguard UK	Several banks shutting down offices because of internal infections


Address
http://www.aircanada.ca/news/resume.html?frominternallink=bannerad
AIR CANADA
Canadian Edition
Welcome
Book Flights
Travel Planning
Traveller Services
Aeroplan
About Air Canada
Air Canada Family
What's New!
Home
My Account
Create an account
View my bookings
Change my bookings
Assistance
Contact Us
Site Map
Search
Logout
AIR CANADA CHECK-IN AND RESERVATIONS SYSTEMS RETURN TO NORMAL OPERATIONS
MONTREAL, August 20, 2003 - Air Canada advises customers that its airport check-in and call centre reservations have returned to normal operations after computer systems were cleared of a worldwide virus impacting many companies including Air Canada.
Customers are requested to arrive at the airport no earlier than regular check-in times in order to avoid contributing to longer queues and wait times :
30 minutes for Rapidair flights between Toronto, Montréal and Ottawa, and between Vancouver, Calgary and Edmonton;
One hour for other domestic Canada flights;
One and a half hours for transborder U.S. flights;
Two hours for international flights.
We regret any inconvenience caused to customers and thank you for your understanding.
Air Canada will provide further updates if the situation changes.
AIR CANADA ADVISES CUSTOMERS OF OPERATIONAL IMPACT DUE TO WORLDWIDE COMPUTER VIRUS

SO HOW COME WE'RE STILL NOT SAFE?

CC image by anonymous9000



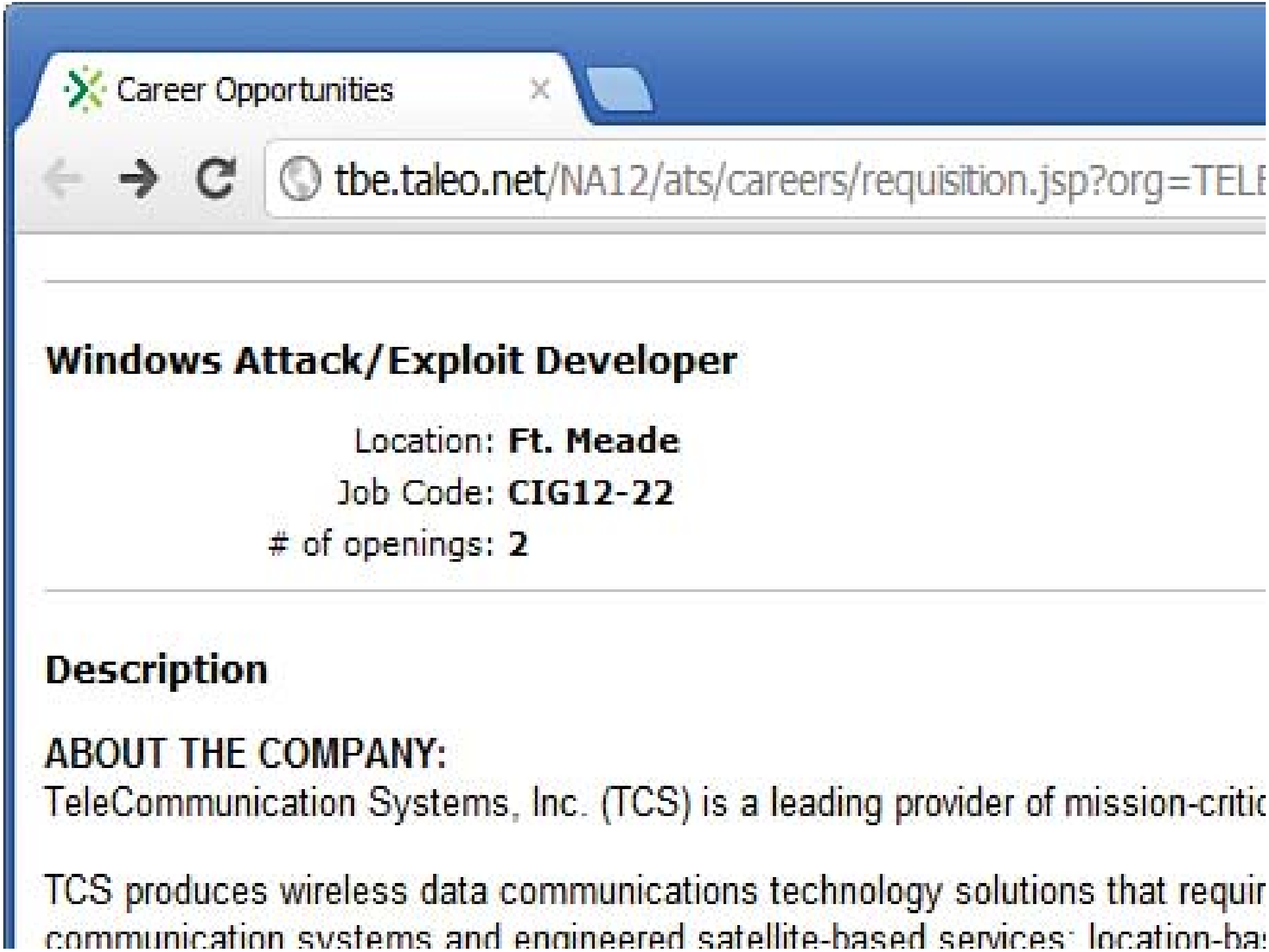

smartclick.org
Media Suffix
Deliver What the Mind Can Dream
HOME
Philosophy
Media Planning
Creative Services
Search Solutions
AD Serving
eCRM
Contact Us
WELCOME TO MEDIASUFFIX...
The internet is widely becoming the hottest advertising and marketing medium in the world. MediaSuffix focuses extremely in the internet segment of advertising. MediaSuffix is ready to show your company how to capitalize on this unbelievable growing market. Don't be left behind.
MediaSuffix is a full one stop service eMedia Solutions. We offer clients an unparalleled range of creative answers to the vary needs of our clients.
We specialize in a broad range of eMedia and integrated marketing services that are customized to build your brand and increase your ecommerce sales.
From media buying and creative to comprehensive ROI tracking, we are professionals experts in


兵信息化素养
事高科技人才

Viewing 1 - 25 of 80 security clearance jobs

exploit offensive

Date	Job Title	Company Name
02/13/12	Cyber System Engineer 2 - HBSS	NORTHROP GRUMMAN
02/13/12	Cyber Systems Engineer 2 - HBSS	NORTHROP GRUMMAN
02/13/12	Cyber Systems Engineer 3 - HBSS	NORTHROP GRUMMAN
02/13/12	Cyber Systems Engineer 3 - HBSS	NORTHROP GRUMMAN
02/13/12	Cyber Systems Engineer 3 CES	NORTHROP GRUMMAN
02/13/12	Cyber Incident Analyst 3 (LIOT CJ)	NORTHROP GRUMMAN
02/13/12	Vulnerability Analyst 3 (LIOT CJ)	NORTHROP GRUMMAN
02/13/12	Information Systems Security Officer...	NORTHROP GRUMMAN
02/13/12	Security Systems Analyst	NORTHROP GRUMMAN
02/13/12	Cyber Counterintelligence	Raytheon
02/13/12	Sr Cyber Incident Responder (LIOT CJ)	NORTHROP GRUMMAN


Career Opportunities
tbe.taleo.net/NA12/ats/careers/requisition.jsp?org=TELE
Windows Attack/Exploit Developer
Location: Ft. Meade
Job Code: CIG12-22
# of openings: 2
Description
ABOUT THE COMPANY:
TeleCommunication Systems, Inc. (TCS) is a leading provider of mission-critic
TCS produces wireless data communications technology solutions that requir
communication systems and engineered satellite-based services; location-ba

General Dynamics Information Technology - Ft Meade, Maryland
Wednesday, November 28, 2012

Information Security Analyst (network exploitation) (TS/SCI Polygraph required) in Ft Meade, Maryland

1 At least five (3) years experience in two (2) or more of the following:

a. Computer Network Exploitation, Computer Network Attack
b.Vulnerability Assessment,
c. Penetration Testing,
d. Incident Response,
e. Network and/or host forensics
f. Cryptanalytic work in military or intelligence community organization,
g.Cryptology work in military or intelligence community organization.

i. Exploit development of personal computer device/mobile device

2 At least three (3) years of experience in three (3) or more of the following:

a. Analysis of host data at rest, including:
i. Microsoft Windows operating systems, system internals, file attributes
ii. Executable file analysis (particularly PE files including dynamic linked libraries)
iii. File Hashing and Fuzzy File Hashing (e.g., ssdeep, fciv, and md5deep)
b
c
d
e

(e.g., Android, Blackberry, iPhone, and iPad.)

f. Industry standard system/network tools (e.g., netcat, netstat, traceroute, rpcinfo, nbtscan, snmpwalk, Sysinternals suite).
g. Exploit development of Microsoft Windows operating systems
h.Exploit development of Linux operating systems
i. Exploit development of personal computer device/mobile device operating systems (e.g., Android, Blackberry, iPhone, and iPad.)
j. Software Reverse Engineering to include use of code disassemblers (e.g., IDA Pro) and debugging unknown code (e.g. Ollydbg)
k.Analysis of code in memory, including analysis of RAM snapshots, Windows crash dump files, and/or Linux kernel dumps
l. SID(S2)/NTOC analysis and production working cyber adversary intrusion set/targets, foreign network intelligence analysis or the identification and extraction of digitally transported information

(Active TS/SCI Polygraph required)

Exploitation Developer

Crystal Clear Technologies, Inc
Posted on: 2/6/13

View company profile

APPLY FOR JOB

Minimum Security Clearance
Top Secret/SCI Clearance - $90,000 plus based on years of experience

Location
Randolph A F B, Texas 78150 (map)

- Workplace: On-Site/Office
- Travel: No Traveling

Crystal Clear Technologies is looking for an Exploitation Developer to work on a highly classified government cyber program in San Antonio, TX. This program involves the design and development of network exploitation and attack tools.

The candidate needs to have expert level knowledge and experience in x86 Assembly Language, Kernel debugging and reverse engineering. Candidate will run current code and if issues are found, examine the code in depth to fix or alter. Will be looking for unknowns in the code. Primarily apps software on Linux boxes. Need to have mature engineering process knowledge and skills in relation to CNA (Computer Network Attack) and CNE (Computer Network Exploitation).

TS/SCI Clearance required, no exceptions

Cyber Software Engineer 2

NORTHROP GRUMMAN

Posted on: 5/14/12

View company profile

APPLY FOR JOB

Minimum Security Clearance

Secret Clearance - Secret

Location

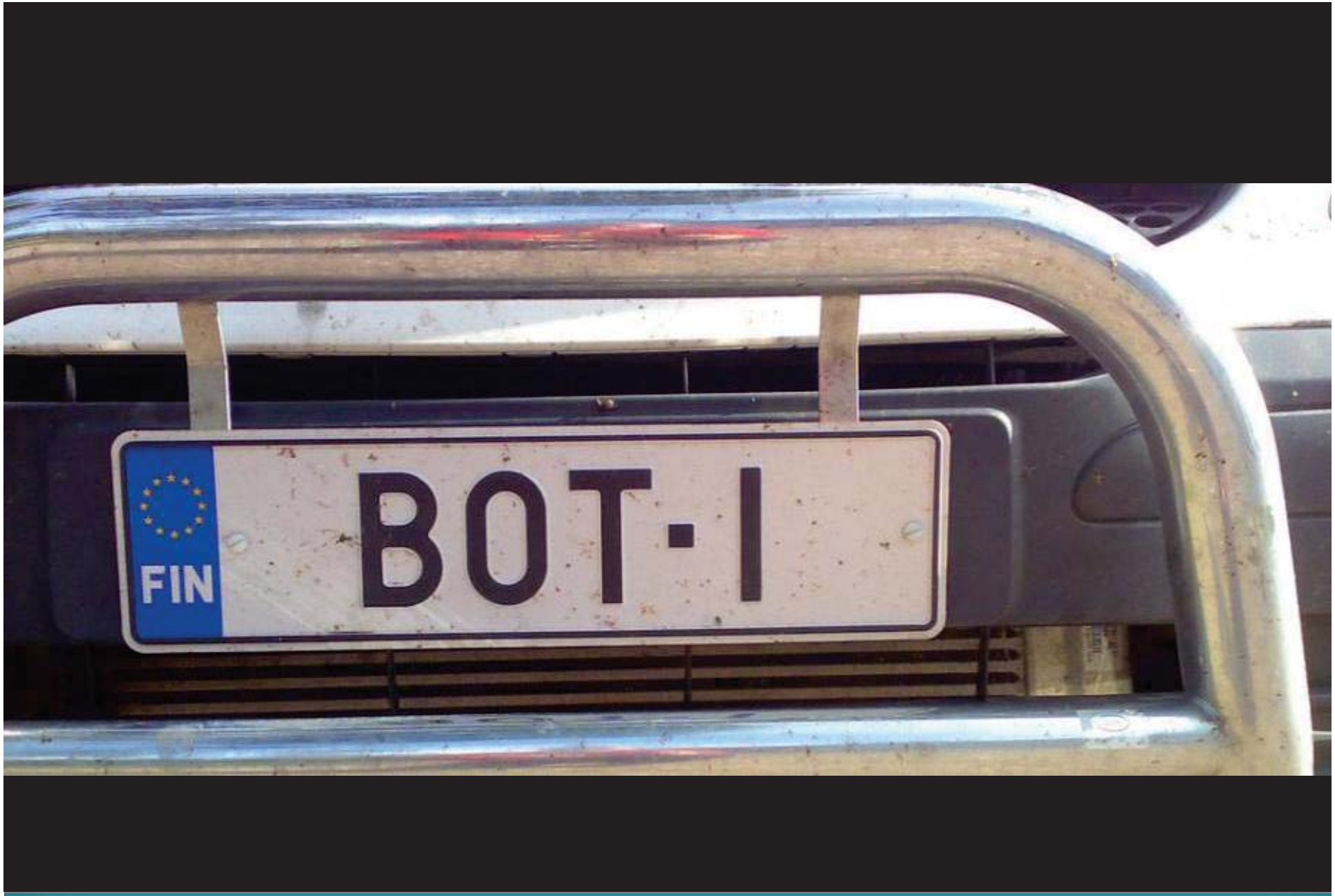
Millersville, Maryland 21108 (map)

- Workplace: Not Specified
- Travel: Not Specified

Northrop Grumman Information Systems sector is seeking a Cyber Software Engineer 2 to join our team of qualified, diverse individuals. This position will be located in Millersville, MD, Colorado Springs, CO, or Sacramento, CA. This exciting and fast paced Research and Development project will plan, execute, and assess an Offensive Cyberspace Operation (OCO) mission. This includes the integration of capabilities such as command linkages, data flows, situational awareness (SA), and command and control (C2) tools..

Roles and Responsibilities:

* Supports the integration of applications for full spectrum Cyber Operations and simulations
* Extends existing simulation tools to include cyberspace components
* Adapts components to a common data integration framework
* Designs, develops, documents, tests and debugs applications software and systems that contain logical and mathematical solutions, GUI components, interface adaptations, or other glue code


FIN
BOT-1


$
Banking Trojans
Ransom Trojans
Credit Card keyloggers
Bitcoin mining
DDoS botnets
Clickfraud


Carberp
Clampi
Cridex
Gataka
Gozi
Oddjob
Ramnit
Shylock
SpyEye
SpitMo
Torpig
URLZone
Zeus
ZitMo

1	4037770002797375	07	2011	779	Donna	Christensen	1224 N 900
2	44779124497087O	04	2011	790	Nancy	Johnson	241 Laurel	La
5	4888940121718221	07	2011	110	Satyam Khanna	1927 West Harrison	St
7	403784002112793 9	07	2011	894	paul kimani muigai	2020 sw broadwa
9	4039954003454175	02	2013	128	Doug	Toburen	1125 N. Juniper
8	4039959477174515	02	2013	125	Brandon D	Dickey	5110 Bob-O-L
7	4870930107935080	10	2011	774	Nyaradzo	Chademunhu	25705 cross
5	4878320074774512	03	2014	922	Dyese Hunt	1552 El Dorado Stree
0	4427271510931707	04	2011	585	Farid	jamshidian	7573 E. Nort
7	5291157334242224	05	2015	934	Lesta	Delaughter	1507 Conrad
3	4303270014720591	09	2014	725	Lagleesa	Harris	1109 Apt.-A Q
4	4257270000917918	12	2014	183	jea s jo	275 Bryn Mawr Ave. E70
7	5108430790019749	07	2014	775	jeanell	burke	139 alison dr
2	5102754887293703	10	2014	472	Lynn	Rosa	530 12th Ave N	Sai
2	4303270013801051	08	2014	753	Mark	albini	2 sanford	Wolcot
8	5300880070310001	04	2011	378	Johnathan	Pevehouse	855 acker
9	4039959177849993	08	2011	104	Schnell	Collins	2411 BROOKDAL
8	4447972177471032	03	2015	417	Jackie	Presley	3558 E 107 ST
2	4828571377879031	01	2015	902	Vernon	Harris	40 Hunt Club bl
4	473790111759342 9	05	2011	489	William	frazier	392 estie gri
3	5291071570942977	11	2014	472	Gerald	Spears	77 Harcourt Ave
1	4509520024074739	07	2015	789	Janusz	mlt	14250 w wigwam blv
4	4303279025818235	05	2015	184	Tim	Orwig	RR1 Box 132	Fairm
0	4227093033747050	08	2014	050	carol	hernandez	5017 57st	l
2	5108430790019749	07	2014	775	jeanell	burke	139 alison dr
0	473790109303209 4	10	2014	042	Angelina	Driver	P.O. Box 243
8	5151580083747784	09	2014	988	Nancy	Garcia	15 armory st	S
9	4807178990070900	07	2014	044	Lavonda lewis	232 Sycamore Avenu
9	4337183017309394	08	2011	513	Jose Vallejos	4102 Colonial Roa
1	4802137097059872	02	2011	317	Donna	Cathcart	43 Douglas Dr.
3	5111750201482434	03	2014	072	denise	gardner	18435 majestic

YOUR COMPUTER HAS BEEN BLOCKED

THE COMMON LAW IS THE WILL OF *Mankind* ISSUING FROM THE *Life* OF THE *People*

THE UNITED STATES DEPARTMENT of JUSTICE

Your IP-address: [redacted]
Your Provider: [redacted]
Location: United States , [redacted]

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article – 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article – 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article – 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

Video-recording: ON

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is $300. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM. ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 5 December 2012. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

green dot MoneyPak

Code: [ ]

1 2 3 4 5 6 7 8 9 0

SUBMIT

Status: Waiting for Payment 47:56:13

Where can I buy MoneyPak

Walmart Save money. Live better. | 7-Eleven | Walgreens | RITE AID PHARMACY | kmart | CVS/pharmacy

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against


BITCOIN
VIRES IN NUMERIS
IN CRYPTOGRAPHY WE TRUST
BITCOIN
WWW.BITCOIN.ORG

F-Secure

Dashboard

Dashboard | Pools | Workers | About

Last updated on : Tuesday, 24th of April 2012 at 16:52:44

Recent work submissions

Worker	Pool	Result	Time
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:42 CEST

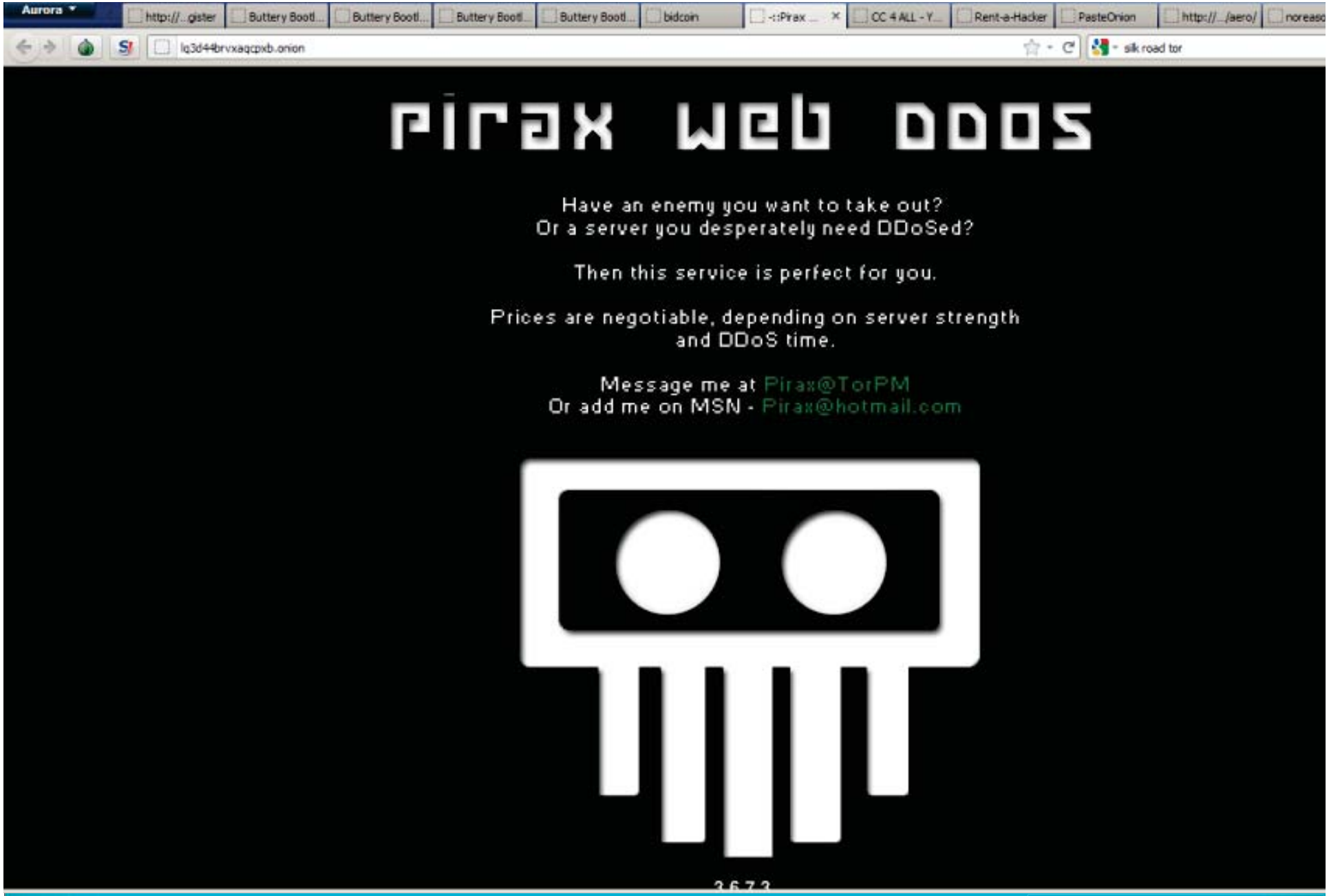
Recent failed work submissions

Worker	Pool	Time
user	BTCguild	24-04-2012 18:52:13 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:08 CEST
user	BTCguild	24-04-2012 18:52:04 CEST

Worker status

Worker	Last work request	Last accepted submission	Shares*	Rejected*	Hashing speed*	Actions
user	At 24-04-2012 18:52:43 CEST from BTCguild	At 24-04-2012 18:52:43 CEST to BTCguild	1483	25 (1.69%)	10615.727 MHash/s	
Totals			1483	25 (1.69%)	10615.727 MHash/s	


DARKNESS
PREMIUM DDoS Bot
With premium admin-panel "Optima"
[From Russia with love]


Aurora
lq3d44brvxaqcpxb.onion
silk road tor
Pirax web DDoS
Have an enemy you want to take out?
Or a server you desperately need DDoSed?
Then this service is perfect for you.
Prices are negotiable, depending on server strength
and DDoS time.
Message me at Pirax@TorPM
Or add me on MSN - Pirax@hotmail.com

Click fraud


Sweden
Finland
Tórshavn
F-Secure Corporation
Tallinn
Norway
Oslo
Stockholm
Estonia
Москва
Moscow
Rīga
Lithuania
Vilnius
Minsk
(Copenhagen)
København
Isle of Man
Dublin
(Warsaw)
Warszawa
Київ
Kiev
United Kingdom
Amsterdam
Netherlands
Berlin
Poland
Ukraine
London
Brussel
Belgium
Germany
(Prague)
Praha
Moldova
Chişinău
Slovakia
Jersey
Paris
Luxembourg
(Vienna)
Wien
Budapest
Hungary
Romania
Austria
Liechtenstein
Bern
Ljubljana
Zagreb
Bucuresti
France
Belgrade
Београд
Serbia
Bulgaria
София
Bosnia and Herzegovina
Приштина
San Marino
Montenegro
Monaco
Podgorica
Скопје
Italy
Andorra
Tirane
Porto (Oporto)
Holy See (Vatican)
Portugal
Spain
Greece
Athens
(Lisbon)
© 2010 Basarsoft
© 2010 Europa Technologies
© 2010 Google
© 2010 Tele Atlas
©2009 Google
49°22'27.47" N 12°50'20.45" E elev 2237 ft
Eye alt 1885.93 mi
Bots
Phishing
Spam
Malware
Worms

F-Secure

Ring0 bundle (Zerokit) for control million-strong botnet

Goto page 1, 2, 3, 4 Next

Post Reply darkode.com Forum Index » Projects

View previous topic
View next topic

Ring0 bundle (Zerokit) for control million-strong botnet

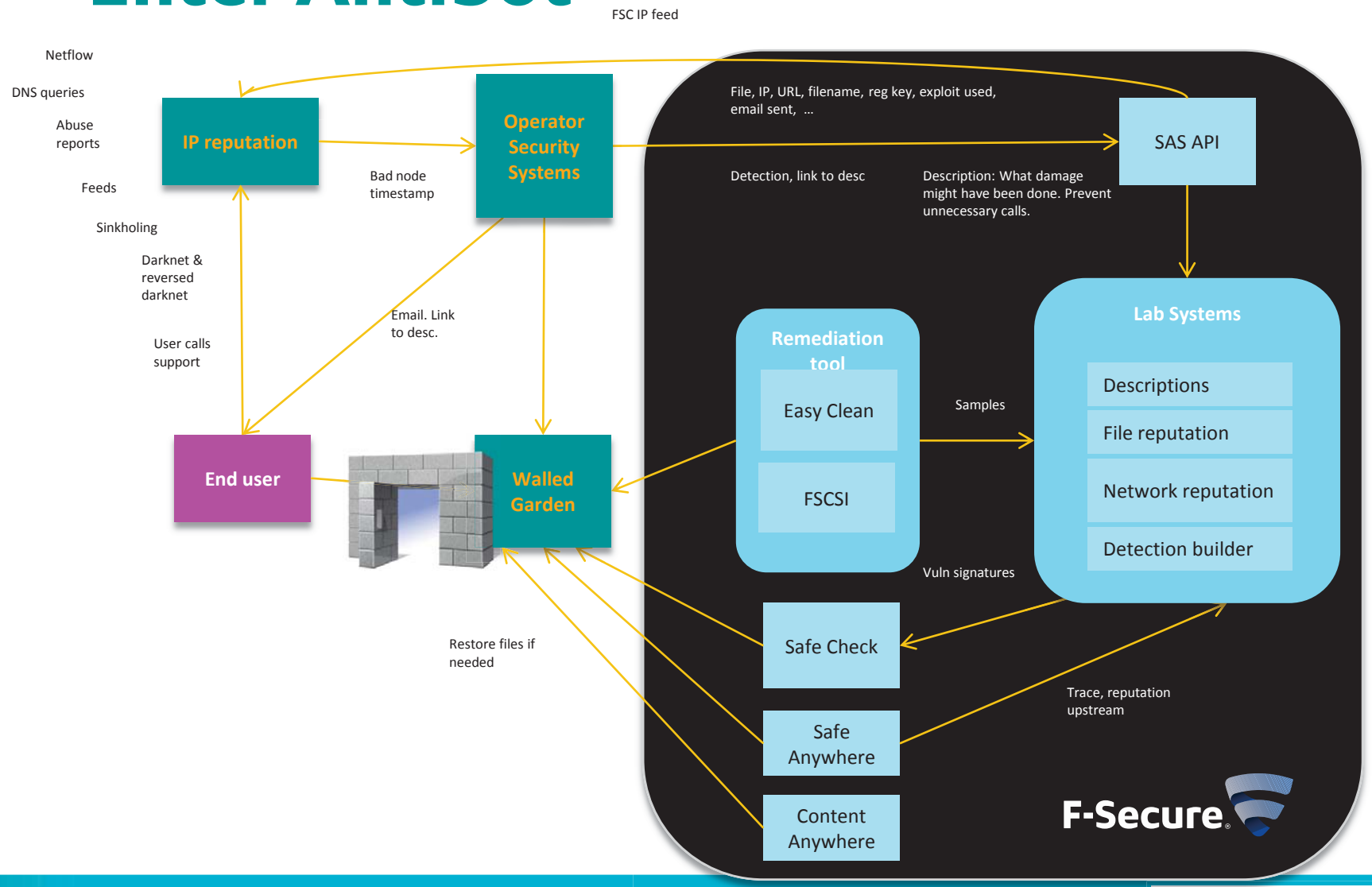
Author	Message
ring0	Ring0 bundle (Zerokit) for control million-strong botnet QUOTE

The bundle consists of:

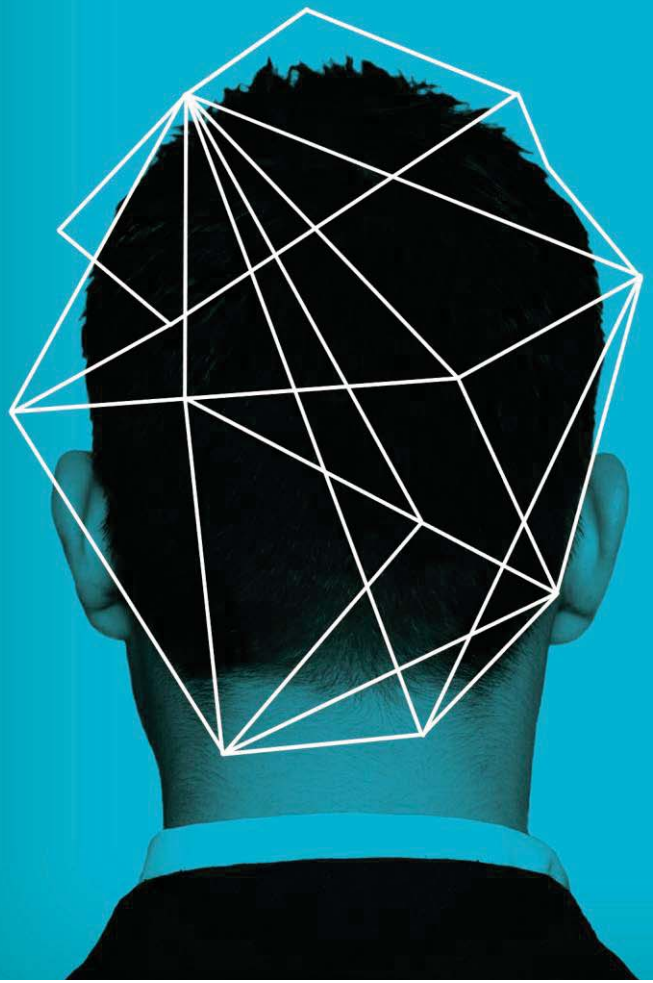
- **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS.
- **Driver.** It is responsible for all infrastructure and implements componental business-logic on the basis of so-called mod (functional unit). That is, the driver is not a legacy driver (monolithic), and consists of the set of mods that allows to operate the bundle with maximum of flexibility, and to protect (hard to reverse), update and expand it.
- **Dropper.** At the current moment it brake out all machines with the patches till January, 8th, 2011, except for XP x32/x64 where reloading is initiated. If the systems distinct from XP have latest updates reloading is initiated as well.
- User friendly Admin Panel.

system without need of crypt.
- Survivability of the bundle, down to a reinstallation of the system.
- All the components are stored outside of a file system and are invisible to OS.
- Intuitively clear interface of admin-panel.
- Protection against the abstraction of Admin Panel.
- Impossibility of detection of the bundle in the working system by any of known AV/rootkit scanner, owing to the use of author's technologies of concealment. The unique opportunity of detection exists only at loading with livecd or scanning of a disk from the other computer. Thus the opportunity of detection is also extremely improbable, as own algorithms of a mutation are used.

Enter Antibot



DEMO TIME!



RSA CONFERENCE 2013

New Ways of Mitigating Botnets

Mikko Hypponen
CRO, F-Secure
@mikko

Security in knowledge

F-Secure

Session ID: BR-R33

Session Classification: Rated R For Adults Only