



Security in knowledge

When State Actors and Cyber Criminals Join Hands



Uri Rivner | Head of Cyber Strategy
BioCatch



Trojan Kits with APT-like tools

Gozi Prinimalka

Онлайн индекс - Проект Блицкриг - Mozilla Firefox

Файл Правка Вид Журнал Закладки Инструменты Справка

Онлайн индекс - Проект Бли... x | Онлайн индекс - Проект Бли... x | Список всех операций x | Готовится релиз лучшего тр... x | Сервис по продаже ботнето... x | +

https://www.██████████.system/admin.py/index?type=system

064003:4976835077 логи:хосты:кукисы:пароли	@ 75.19.35.██████████ (001:15:23:03 96% good)	Placentia, CA, 714 (PST)	1 2 3 4 x 6 Z	прокси: etrade <i>paypal</i> x
064003:4183383737 логи:хосты:кукисы:пароли	@ 72.211.169.██████████ (001:01:45:11 96% good)	Sierra Vista, AZ, 520 (MST)	1 2 3 4 x 6 Z	прокси: etrade <i>paypal</i> x
064003:4318197086 логи:хосты:кукисы:пароли	@ 173.11.171.██████████ (000:02:44:58 96% good)	Spring, TX, 281 (CST)	1 2 3 4 x 6 Z	Чек: etrade <i>paypal</i> x
064003:1994318292 логи:хосты:кукисы:пароли	@ 50.27.202.██████████ (000:04:40:04 96% good)	Tyler, TX, 903 (CST)	1 2 3 4 x 6 Z	Прокси: etrade <i>paypal</i> x
064003:6098970847 логи:хосты:кукисы:пароли	@ 71.59.210.██████████ (001:15:23:03 96% not bad)	Portland, OR, 503 (PST)	1 2 3 4 x 6 Z	x
064003:6617117088 логи:хосты:кукисы:пароли	@ 75.0.224.██████████ (001:05:47:41 96% good)	Corpus Christi, TX, 361 (CST)	1 2 3 4 x 6 Z	прокси: chase <i>paypal</i> x
064003:4701119690 логи:хосты:кукисы:пароли	@ 71.149.255.██████████ (000:20:38:26 97% good)	Monterey, CA, 831 (PST)	1 2 3 4 x 6 Z	прокси: etrade; <i>paypal</i> x
064003:9234121239 логи:хосты:кукисы:пароли	@ 98.67.251.██████████ (001:15:23:00 97% good)	Coushatta, LA, 318 (CST)	1 2 3 4 x 6 Z	чек: Schwab, Etrade <i>paypal</i> x
064003:6769330797 логи:хосты:кукисы:пароли	@ 50.132.106.██████████ (001:15:22:51 98% not bad)		1 2 3 4 x 6 Z	x
064003:5641193330 логи:хосты:кукисы:пароли	@ 69.238.26.██████████ (001:15:22:51 100% good)		1 2 3 4 x 6 Z	x
064003:6117851329 логи:хосты:кукисы:пароли	@ 216.175.62.██████████ (001:15:23:02 100% good)	Sullivan, IL, 217 (CST)	1 2 3 4 x 6 Z	прокси: etrade <i>paypal</i> x

Найти: bad | Следующее | Предыдущее | Подсветить все | Учесть регистр



VncFox 2012 - Citadel Software

Citadel VNC Plugin - \$495 USD / €375

VNCFox, full version adapted to the Citadel control panel

- Enables data collection from specific PCs (for example, those belonging to companies) and from accounts of interest, placing it into a separate database via a separate script
- Create a triggered instant connection to a specific BotID, and have the VNC connection automatically established whenever the bot comes online

CONFIG
vncserver

login

password

host

port

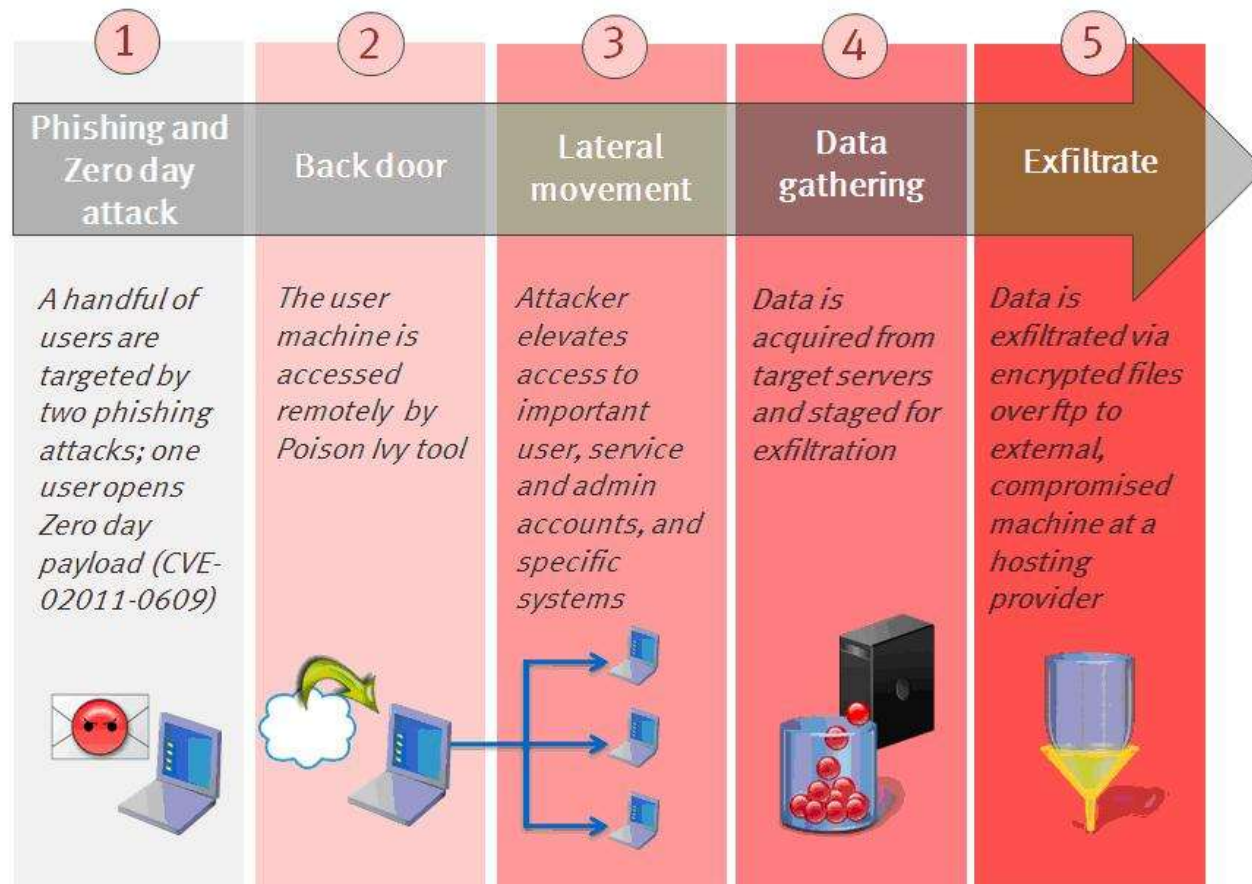
rcpt

All accounts: 12 Live accounts: 12 (%100) Dead accounts: 0 (%0)

AK (vec)	BOTID	OS	TYPE	Z	SET	ACC	AGENT	PRIO	CNO	IBR	HEED
61 sec	TRIPLE-C_707576894190172	XP SP 1	22-12-2011 11:52:38	216	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 24900	ON	ON
53 sec	STORAGE_84DF61167175CC2	XP SP 2	25-12-2011 16:29:07	2300	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 24900	ON	ON
53 sec	STORAGE_84DF61167175CC2	XP SP 2	25-12-2011 16:21:36	2300	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 23366	ON	ON
116 sec	CHCLITO-PC_74DE81E83F5149E	Seven	04-12-2011 10:25:44	436	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 24744	ON	ON
212 sec	700R-248AM776GV_7BF1A2E18589A134	XP SP 3	22-12-2011 13:13:46	609	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 29139	ON	ON
221 sec	USER-TOSH_7F1A2E1840075A16	Seven (64)	20-12-2011 18:34:19	593	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 27141	ON	ON
117 sec	ADMIN-PC_7BF1A2E184099624	XP SP 3	19-12-2011 21:49:22	1304	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 20048	ON	ON
147 sec	ADMIN-PC_7BF1A2E184099624	XP SP 3	19-12-2011 21:39:27	1306	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 27509	ON	ON
147 sec	ADMIN-PC_7BF1A2E184099624	XP SP 3	19-12-2011 21:35:23	1306	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 25079	ON	ON
147 sec	ADMIN-PC_7BF1A2E184099624	XP SP 3	19-12-2011 21:48:52	1306	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 23939	ON	ON
170 sec	CHELSEA-LAPTOP_4AD73E34UC31C88C	Vista SP 2	19-12-2011 21:26:34	359	100%	100%	tr	SET	bot_tc_add vnc 192.168.1.100 22643	ON	ON
			19-12-2011					SET	bot_tc_add vnc 192.168.1.100 21779		





Other Famous RATs



Recent RAT Infestation: Israeli Institute for National Security Studies

SIGN UP | ABOUT INSS | EXPERTS | MEDIA | PRIZES | CONTACT | LOGIN | עברית




Interview with Amos Yadlin, on Canadian national television

Site Search

[Advanced Search](#)

- Research
- Publications
- Events
- Programs
- Israel's National Security
- ME Military Forces
- Israeli Public Opinion
- Links



Following Egypt's Constitutional Referendum: Polarization and Collapse: Discourse on the Egyptian Social Networks, January 2013

Udi Dekel and Orit Perlov (January 9, 2013) present some of the principal sentiments, foremost among them social polarization and collapse, voiced on the Egyptian social networks following the recent constitutional referendum.

[more info](#)

Has Operation Pillar of Defense Enhanced Israel's Deterrence?

Zaki Shalom (e-International Relations, January 6, 2013) discusses various aspects of Operation Pillar of Defense, focusing on the potential contribution of the campaign to Israeli deterrence.

[more info](#)

New INSS Memorandum: In the Aftermath of Operation Pillar of Defense

The essays by INSS researchers compiled in this volume offer initial assessments of various aspects of Operation Pillar of Defense, launched by Israel in the Gaza Strip in November 2012.

[more info](#)

New INSS Insight: The EU Draws a Red Line on Israeli Settlements


Shimon Stein (January 1, 2013) analyzes the increasingly harsh European tone in response to Israel's recent decision to accelerate

Challenges of Warfare in Densely Populated Areas: Conference at INSS, February 6, 2013

Conference sponsored by INSS and the International Committee of the Red Cross (ICRC)
Click here to register for the conference.

New Memorandum: In the Aftermath of Operation Pillar of Defense

The essays compiled in this volume offer initial assessments of various aspects of Operation Pillar of Defense, launched by Israel in the Gaza Strip in November 2012.





When States control Botnets

State-owned Botnet

KrebsonSecurity

In-depth security news and investigation



ABOUT THIS BLOG

ABOUT THE AUTHOR

302-DIRECT-MEDIA-ASN

8e6 Technologies, Inc.

AAPT AAPT Limited

ABBOTT Abbot Labs

ABOVENET-CUSTOMER – Abovenet Communications, Inc

ACCNETWORKS – Advanced Computer Connections

ACEDATACENTERS-AS-1 – Ace Data Centers, Inc.

ACSEAST – ACS Inc.

ACS-INTERNET – Affiliated Computer Services

ACS-INTERNET – Armstrong Cable Services

ADELPHIA-AS – Road Runner HoldCo LLC

Administracion Nacional de Telecomunicaciones

AERO-NET – The Aerospace Corporation

AHP – WYETH-AYERST/AMERICAN HOME PRODUCTS

AIRLOGIC – Digital Magicians, Inc.

AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services

AIS-WEST – American Internet Services, LLC.

AKADO-STOLITSA-AS _AKADO-Stolitsa_ JSC

ALCANET Corporate ALCANET Access

ALCANET-DE-AS Alcanet International Deutschland GmbH

ALCATEL-NA – Alcanet International NA

ALCHEMYNET – Alchemy Communications, Inc.

Alestra, S. de R.L. de C.V.

ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services Pvt. Ltd.,Alliance Gateway

AS,Broadband Services Provider,Kolkata,India

ALMAZAYA Almazaya gateway L.L.C

AMAZON-AES – Amazon.com, Inc.

AMERITECH-AS – AT&T Services, Inc.

Advertisement

NEW! A POWERFUL APP FOR
PROTECTING ONLINE TRANSACTIONS
AND ACCOUNTS FROM EXPLOITS



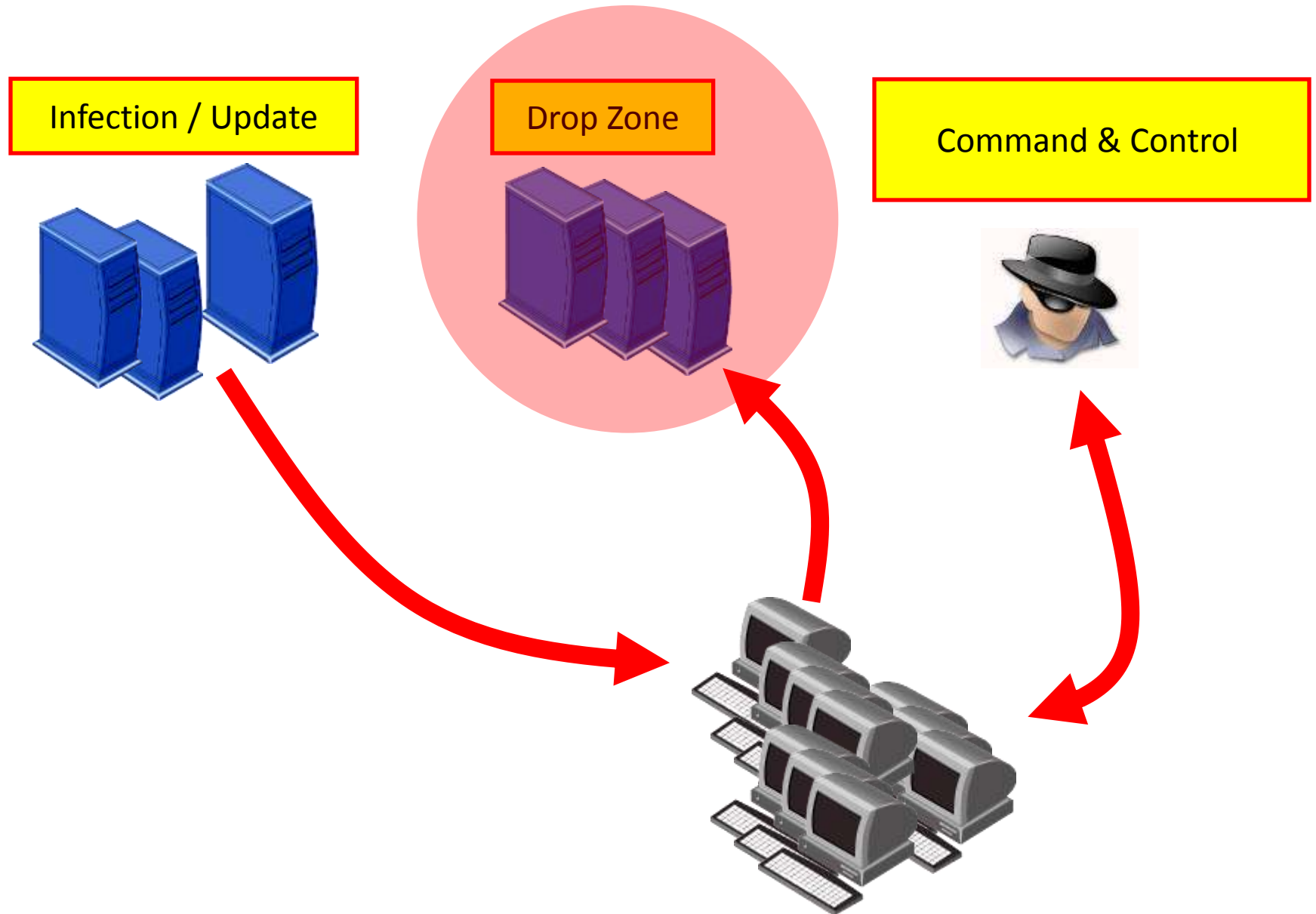
Recent Posts

[Zero-Day Java Exploit Debuts in](#)

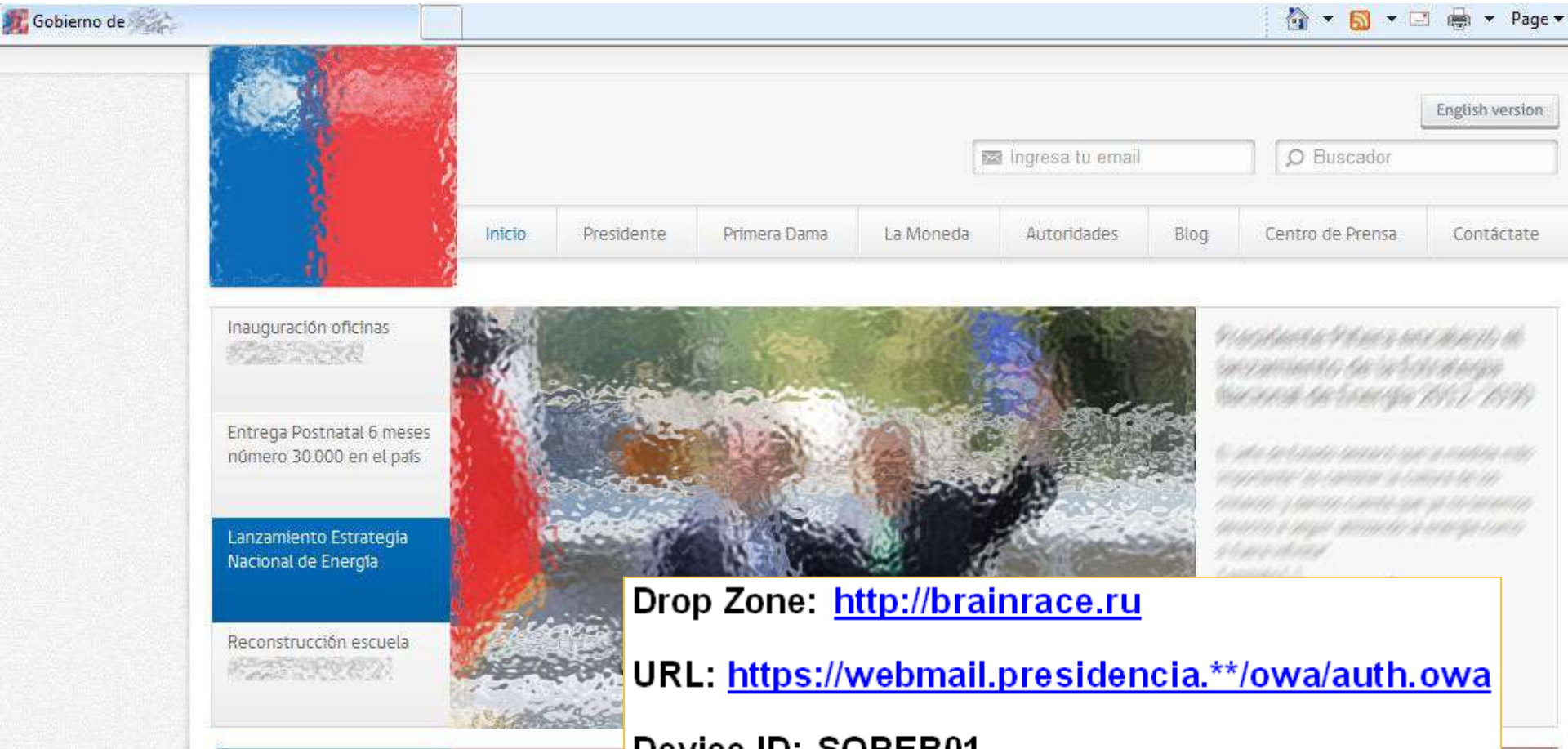


Government, Military PCs for Sale

Trojan Infrastructure



The Presidential Office



Drop Zone: <http://brainrace.ru>

URL: https://webmail.presidencia.*/owa/auth.owa

Device ID: SOPER01

Network Name: PR*****\monitores

User name=PR*****/SEGURIDAD

password=SEGURIDAD****

Atomic Energy in South East Asia

Official Website Atomic Energy Licensing Board

Anniversary (1985 - 2010) 25 AELB ATOMIC ENERGY LICENSING BOARD

Home About AELB Procedures Licenses Applications

Quality Policy
Client Charter
Performance of Client Charter
Online Transaction
Notices for Client
Nuclear Emergency Team (NET)
Registration for RPO Examination (RPO)
Timetable for RPO Examination 2012
RPO Course Schedule 2012
Public Complaints
Feedback

under the Prime Minister's Office
body for the implementation
the Ministry of Science, Technology and Innovation

URL: [https://mail.aelb.gov.**/owa/auth.owa](https://mail.aelb.gov.my/owa/auth.owa)
Device ID: IR***-***-PC
Network ID: AELB\ir***
username=ir***@aelb.gov.**
password=ir***5105is

T PROCEDURES
TIVE SOURCES

MOHD. EFFENDI MOHD. I
Licensing Division
Atomic Energy Licensing Board (AELB)
Ministry Of Science Technology & Innovation
E-mail : i@aelb.gov.

Foreign Space Agency

LinkedIn

Enrico [redacted]
Defense & Space

Join LinkedIn and access Enrico [redacted]

As a LinkedIn member, you'll join 150 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and Enrico [redacted] know in common
- Get introduced to Enrico [redacted]
- Contact Enrico [redacted] directly

Enrico [redacted] Overview
Connections 117 connections

Enrico [redacted]'s Skills & Expertise

Space Systems Systems Engineering Requirements Engineering
Testing Validation Assembly



Url: https://ice.sso.***.int/ICSLogin/auth-up

Time Stamp: 2012-01-05T19:47:12Z

Device Name: ***LE102971

Network Name: ***AD\Enrico*****

User name: e*****

Password=[kedkedede](#)

IP: [***.***.4.126](#)

IP Location: **** **** Space Operations Center

Resolve Host: [***-***-4-126.hq.***.int](#)

- Welcome to
- News a
- Establishme
- and facilitie
- Careers at
- Education w
- Business wit
- activiti
- Observing t
- Human Spa
- Launchers
- Navigation
- Space Science
- Space Engineering
- Space Operations & Situational Awareness
- Technology
- Telecommunications & Integrated Applications



28 Februa
planet wit
programm
M
of the sat

Government, Military for Sale



Posts: 2
Joined: 12 Jan 2012 19:49
Reputation point: 0



Military and Government

by  13 Jan 2012 02:52



Ok I am selling government and military logins, anything you want access to, I can get it for you, just pm me the links/ip address etc and I will get you the logins/databases/documents/ftp servers/ or whatever it is that you want.

There is no fixed price as the difficulty of getting access/classification etc has to be taken into consideration, like I said if you are interested just pm me with the ip address etc and what you want, I will then give you the price and how long it will take.

To show you I am not fucking you around check out my video:



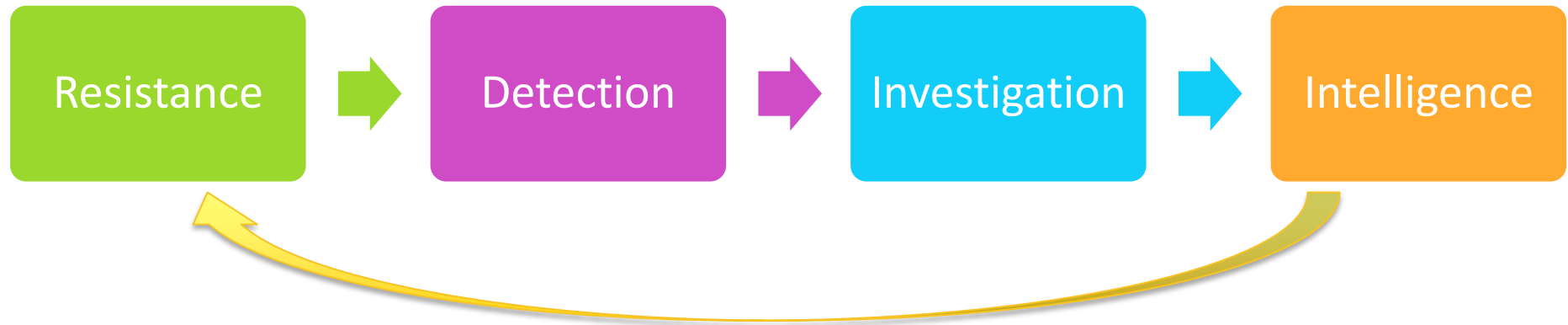
I hope admins/mods don't mind me posting my video link.





New Defense Doctrine

Fighting Advanced Threats



Summary

- ▶ Cyber Criminals have access to APT-grade tools
- ▶ Military Intelligence has access to massive Botnets
- ▶ Financially motivated hackers sell .gov, .mil accounts
- ▶ New Defense Doctrine needed

Q&A

Got any questions? Send me a
LinkedIn invitation (Uri Rivner)

