

A Eficiência na Resposta a Ameaças

Tecnologias focadas para respostas direcionadas (e confiantes).

10º EIN /
Cyber Intelligence e Situational Awareness no Ciberespaço
29 Abril 2016

Rui Diogo Serra
Sr Product Marketing Manager

Tecnologias focadas para
respostas direcionadas

Nationwide Defense Organizations



CyberDefesa

~13000M

Connected
devices 2015

~ 35% de
7000M

Pessoas online
2015

15 Triliões de
Gigabytes

Total Dados

In: NATO, National Cybersecurity
framework, 2016
The Hague HCSS Report 2015

Nationwide Defense Organizations

CyberDefesa

> Mandatos

Cyber Warfare

**& Militar, Counter,
Intelligence, etc..**

**Proteção de CIS
das
Infraestruturas
Críticas**

**Computer
Incident
Response**

& Resposta a crises

...

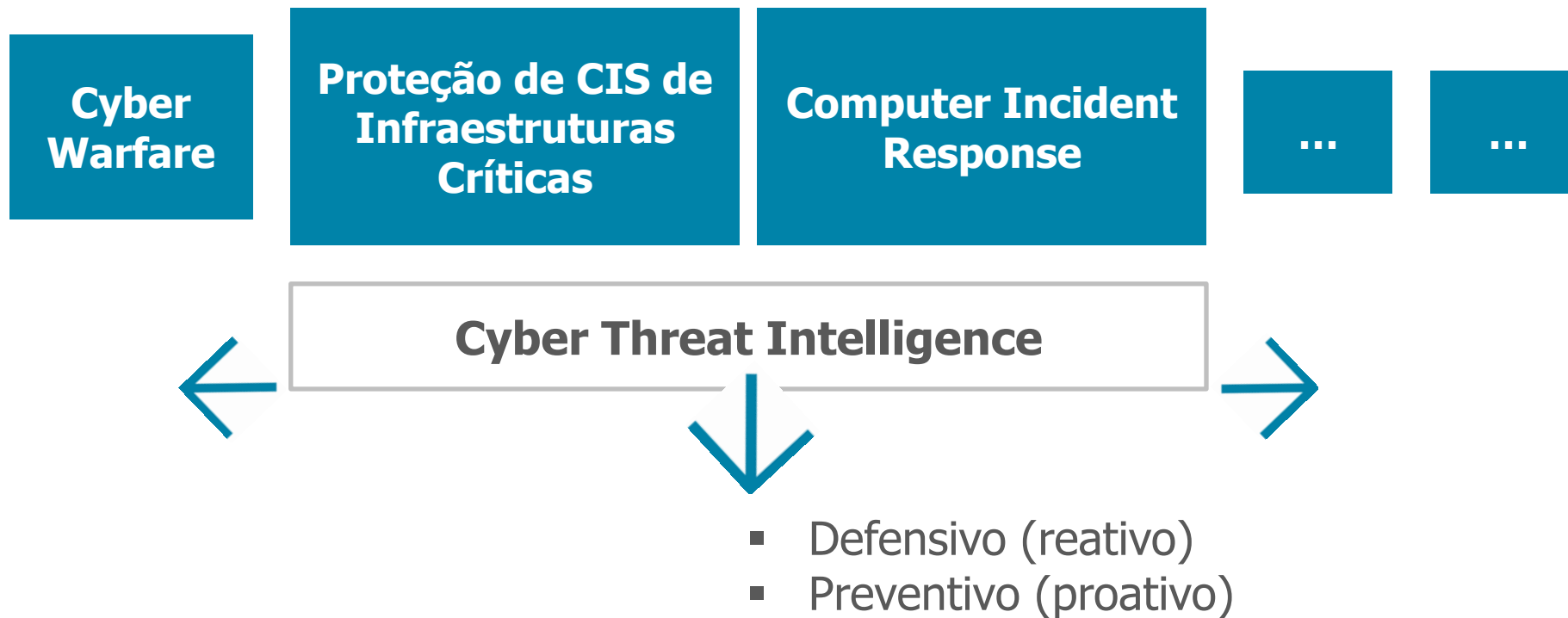
...

Nationwide Defense Organizations

CyberDefesa



Operacional



Nationwide Defense Organizations

CyberDefesa

> Objetivo

**Proteção de
Infraestruturas
Críticas**

**Computer Incident
Response**

Cyber Threat Intelligence



Situational Awareness & Response

Eficiência na Resposta a Ameaças

**Cyber
Threat Intelligence**



**Situational Awareness
& Response**

**Como obter uma *threat perspective*
de diferentes geografias, e de diferentes
“portfolios”**

E como operacionalizar estes dados?

(*) Portfolios: Critical Infrastructures vs. Threat Landscape (País) vs. Threat Landscape internacional

Eficiência na Resposta a Ameaças

Cyber
Threat Intelligence



Situational Awareness
& Response

Atividade



Como obter uma *threat perspective*
de diferentes geografias, e de diferentes
“portfolios”

E como operacionalizar estes dados?

Foco

Direção

Confiança

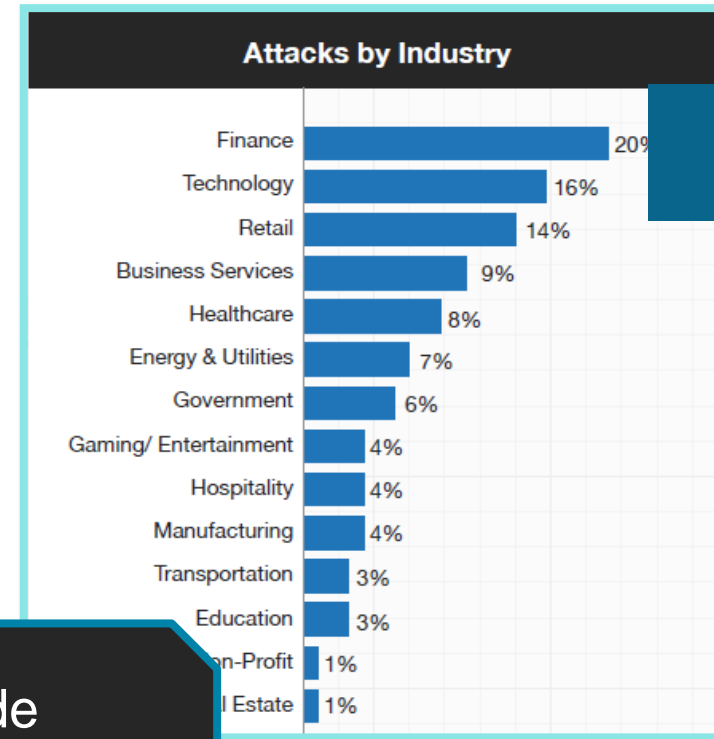
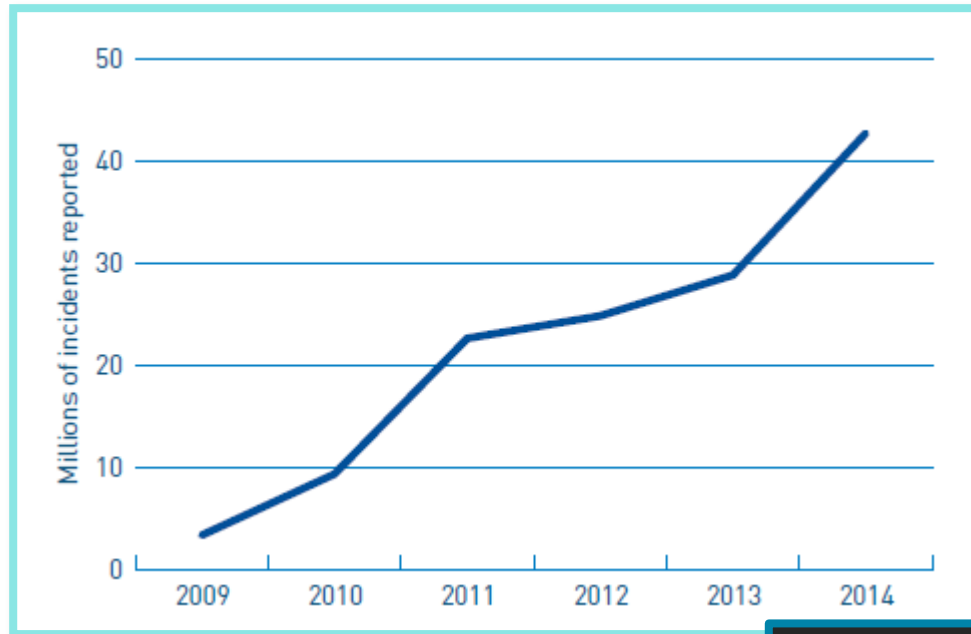
Mindset

Tecnologias Focadas

Cyber Threat Intelligence



Situational Awareness & Response



Foco

50M de
Cyber Incidentes /
ano

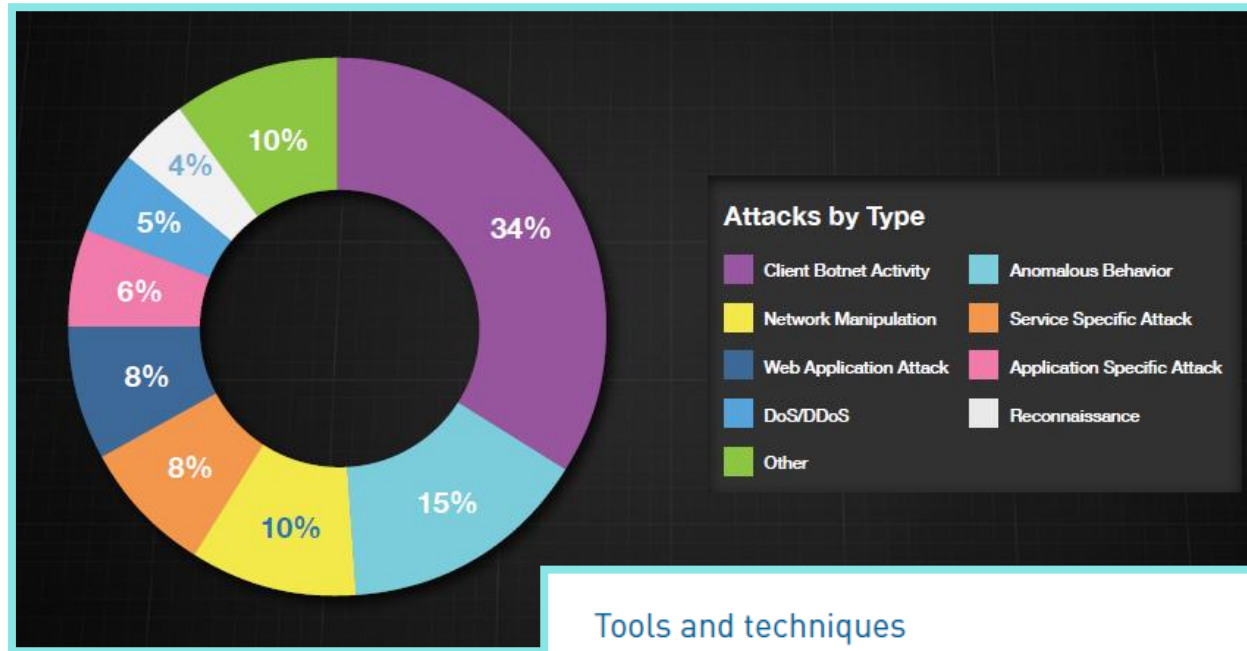
IV: The Hague HCSS
Report 2015, PWC 2015

Tecnologias Focadas

Cyber
Threat Intelligence



Situational Awareness
& Response



Foco

Tools and techniques

- Most reports point to malware, worms and trojans as most prevalent attack techniques used.

IN: NTT Global Threat report, 2014

Uma Framework de Situational Awareness & Resposta a Incidentes:



Ingestão e correlação de CTI em tempo real



Informação **confiável, profunda** sobre o ataque
(vector, campanha, sistema, organização)



Capacidades de **Situational Awareness**:
Reporting, monitorização, data mining, que permitam identificação rápida de anomalias, tendências, padrões



Portfolio vs. Threat Landscape
Setores, Indústrias, Geografias / nacional vs. internacional

REAL-TIME
BOTNET ACTIVITY
LANDSCAPE

LIVE GLOBE

DASHBOARD

SOUTH AMERICA

ALL COUNTRIES

BOTNETS

ALL BOTNETS

SELECT BOTNET FAMILY

Search for a Botnet... X

ALL BOTNETS

ADMOGO

ADPEAK

ADWARE

ADVANCE

ALUREON

ANDROIDLUCKY

ANDROIDSMS

ANDROMEDA

AUTOIT

BAMITAL

BANJORI

BAYROB

BEDEP

BERROF

BETABOT

CARBANAK

CARUFAX

CLICKFRAUD

COINMINER

SOUTH AMERICA CURRENT TOTAL

ALL BOTNETS

CONNECTIONS

353

INFECTIONS

202,333

TOP COUNTRIES

BRAZIL	147.99	77,433
COLOMBIA	54.65	20,725
PERU	47.87	24,615
ARGENTINA	34.91	34,543
VENEZUELA	29.92	45,709

TOP CITIES

LIMA	23.54
LA PAZ	13.57
MEDELLÍN	13.37
QUITO	12.37
BOGOTÁ	8.98

anubisnetworks™
a BITSIGHT® company

RESUME

ANIMATION

+

-

🐞

INFECTIONS EVOLUTION

OLD  NEW

anubisnetworks™
a BITSIGHT® company

GLOSSARY

ABOUT

SHARE THIS

DISCLAIMER

© 2015 ANUBISNETWORKS. ALL RIGHTS RESERVED.

Anubis > Threat Intelligence



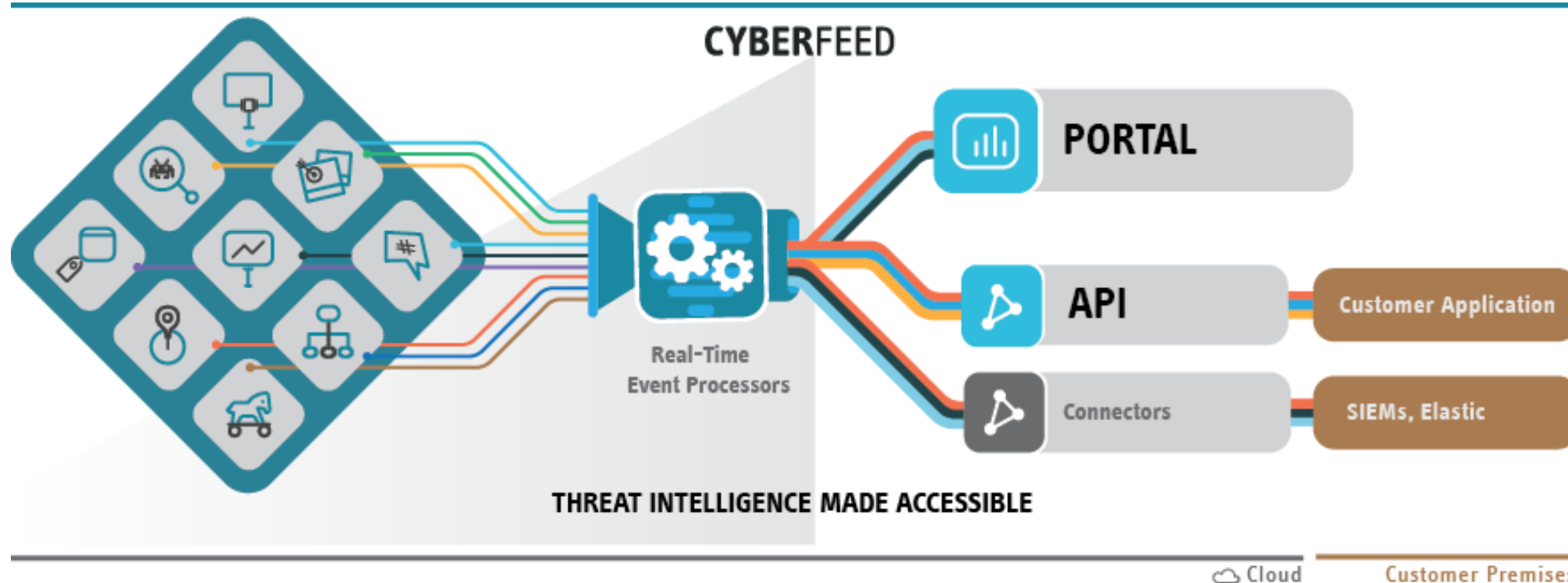
Cybersecurity infrastructure + Security Labs



Real-time Events > **infections and vulnerabilities**

+ **Depth and Breadth:**

- sectors, companies and industries,
- malware remediation and severity, communication
- payloads, forensics, CVEs, IOCs.



Cloud

Customer Premises

Threat Intelligence Platform

CYBERFEED PORTAL PORTFOLIO **COMPANIES** ? ⚙️

⇅ **17** Saperix, Inc. DASHBOARD EVENTS **FORENSICS** COMPANY DOWNLOAD AS: CSV

FILTER EVENTS FORENSICS FOR THE LAST 7 DAYS

SEARCH
Enter search term...

TIME RANGE
24h **7d** 30d 6m

INFECTION TYPES

- All **596**
- Genieo **388**
- InstallMonster **65**
- Sality **64**
- Defaulttab **47**
- Adware **16**

SHOW ALL (8)

IP ADDRESSES

- All **596**
- 24.12.168.195 **251**
- 24.6.18.168 **77**
- 24.12.168.91 **65**
- 24.6.28.217 **64**
- 24.6.25.205 **31**

SHOW ALL (17)

COUNTRIES

DATE/TIME	IP ADDRESS	INFECTION TYPE	SINKHOLE	COUNTRY
2016-04-11 16:54:19	24.12.168.195:63470	Genieo Trojan	195.22.28.199:80 live-genieo-feed.com	United States
2016-04-11 16:14:18	24.12.168.195:63042	Genieo Trojan	195.22.28.197:80 live-genieo-feed.com	United States
2016-04-11 15:49:12	24.6.25.205:50460	Defaulttab Trojan	195.22.28.197:80 update.searchcu	United States
2016-04-11 15:34:17	24.12.168.195:62061	Genieo Trojan	195.22.28.198:80 live-genieo-feed.com	United States
2016-04-11 15:26:00	24.12.168.91:53421	InstallMonster Trojan	195.22.28.198:80 lb.mspb4-01.com	United States
2016-04-11 15:22:15	24.12.168.91:53411	InstallMonster Trojan	195.22.28.198:80 lb.mspb4-01.com	United States

DETAILS

INFECTION ALIASES
Potentially Unwanted Application
Potentially Unwanted Program

INFECTION DESCRIPTION
Genieo is a potentially unwanted application which changes the default homepage of a browser and inject ads and sponsored links into search results.

RISKS
Resource Abuse

TARGETED PLATFORM
MacOSX

REMIEDIATION INSTRUCTIONS
symantec.com

maltracker Dashboard Analyses Samples C2 Hosts Submit Search ⚙️

Home / Dashboard

LASTEST ANALYSES

- fb3ce349d2636683036f31770c87b395
http://www.bhelvastu.com/downloader/lib/image/autoloac
Completed on: 2016-04-29 02:57:57
- 7a5aea34d2ff913252cee8f01a2d90b7
http://prime-travels.net/awa/
Completed on: 2016-04-29 02:57:55
- 795cd694659524e98c54d935e5ca40ac
http://www.campusfrancemaroc.info/verificationpurpose
Completed on: 2016-04-29 02:57:54
- afbe0dc9ffc062d3fb1b331b5c7a6d9
http://www.exclusiveprint.co.uk/massounia/amzaon/6b2
Completed on: 2016-04-29 02:57:54
- 00cdb832132c015cecc011c3094409b2
http://www.mnest.co.id/usaaweb2.php
Completed on: 2016-04-29 02:57:43
- d21487ff2c50e5e29cf5b2850ff70620
http://digitalpolo.com.br/wp-includes/js/idrop-boxx/2d...
Completed on: 2016-04-29 02:57:43

LASTEST C2 HOSTS

- rsyqtxb.uk
2016-04-29 01:28:14 | 178.162.203.202 | Leaseweb Deutschland GmbH
- alpha.protonhost.net
2016-04-28 18:42:11 | 149.202.91.58 | OVH SAS
- www.iiamo.com.au
2016-04-28 16:26:19 | 117.55.235.17 | UberGlobal Pty Ltd
- ip_107.170.20.33
2016-04-28 14:26:12 | 107.170.20.33 | Digital Ocean, Inc.
- htankds.info
2016-04-28 14:26:12 | 91.219.31.18 | Limited Liability Company DataHarbour

TAGS

avc pua necurs waldek razy
installmonetizer **phishing**
kryptik locky ransom adware
bundler application shouqu
malicious y5 dridex somoto
malware **inbox** pup
qjwmonkey toolbar filecoder

TOTAL ANALYSES
1214981

TOTAL SAMPLES
1400974

SUSPICIOUS HOSTS
24469

Cyberfeed Live Analytics

REAL-TIME
BOTNET ACTIVITY
LANDSCAPE

LIVE GLOBE DASHBOARD

RESUME ANIMATION

+

-

INFECTIONS EVOLUTION

OLD NEW

EUROPE

PORTUGAL

BOTNETS

ALL BOTNETS

PORTUGAL ALL BOTNETS

CONNECTIONS

277

TOP PORTUGAL CITIES AFFECTED

- FUNCHAL
- VIZELA
- OLIVEIRA DE AZEISEIS
- ALGÉS
- BARCELOS

OTHER BOTNETS IN PORTUGAL

- NYMAIM
- CARUFAX
- ZEUS
- ADWARE
- JOINKJOT

GLOSSARY ABOUT SHARE THIS DISCLAIMER

© 2015 ANUBISNETWORKS. ALL RIGHTS RESERVED.

anubisnetworks™
a BITSIGHT company

Cyberfeed
threat intelligence dashboard

2016.04.29 03:05:42
9 of 17108 events/s

Botnets in the USA

top infected cities in us

springfield	20.6
new york	10.4
las vegas	9.5
san antonio	8.7
new hyde park	8.2
saint louis	8.1
mesquite	7.3
brooklyn	6.4
los angeles	6.2

top botnets in country (nl)

sinowal	82.2%
rerdom	4.0%
installmonster	2.7%
zeus	1.4%
genieo	1.4%
admogo	0.9%
spyapp	0.9%
joinkjot	0.9%
necuris	0.9%

default portlet

dnslog	30.7%
banktrojan	30.6%
rbim	20.3%
dnsmalware	15.3%
spike-prod	1.2%
repchanges	1.1%
trap	0.9%
spike3	0.4%
dmarsensus	0.1%

default portlet

banktrojan	2.8k
dnslog	2.8k
rbim	1.8k
dnsmalware	1.4k
spike-prod	103.8
repchanges	99.1
trap	76.5
spike3	30.1
dmarsensus	0.2

default portlet

banktrojan	30.7%
dnslog	30.6%
rbim	20.2%
dnsmalware	15.3%
spike-prod	1.2%
repchanges	1.1%
trap	0.9%
spike3	0.4%
dmarsensus	0.1%

Reporting & Monitoring

CYBERFEED PORTAL | PORTFOLIO | COMPANIES

17 Saperix, Inc. | DASHBOARD | EVENTS | FORENSICS | COMPANY | DOWNLOAD AS: PDF

EVENTS

Last 7 days: **17** (6% less)

Last 24 hours: **11** (8% less)

ACTIVE IP ADDRESSES

Last 7 days: **17** (6% less)

Last 24 hours: **11** (8% less)

EVENT STATUS [Go to events page](#)

New: **15**

Acknowledged: **2**

MOST ACTIVE INFECTIONS • Last 7 days

INFECTION TYPE	# IP	DENSITY	BEFORE
Genio	5	0.1%	0.1%
Defaulttab	4	<0.1%	<0.1%
Viknok	2	<0.1%	<0.1%
Adware	2	<0.1%	<0.1%
Bedep	1	<0.1%	0%
Conficker_B	1	<0.1%	0%
InstallMonster	1	<0.1%	<0.1%
Sality	1	<0.1%	<0.1%

MOST ACTIVE IP ADDRESSES • Last 7 days

IP ADDRESS	ATTRIBUTED TO
24.12.168.195	
24.6.18.168	
24.12.168.91	
24.6.28.217	
24.6.25.205	
24.6.20.201	
24.6.23.66	
24.6.27.44	
24.6.28.21	
24.12.170.105	

INFECTION DISTRIBUTION • Last 7 days

LATEST EVENTS • Last 7 days

LAST SEEN	IP ADDRESS	ATTRIBUTED TO
2016-04-11	24.12.168.195	
2016-04-11	24.6.25.205	
2016-04-11	24.12.168.91	
2016-04-11	24.6.28.217	
2016-04-11	24.6.20.201	
2016-04-11	24.12.170.202	
2016-04-11	24.6.18.168	
2016-04-11	24.6.30.83	
2016-04-11	24.6.20.144	
2016-04-10	24.6.25.20	

Daily Cyberfeed Digest | Inbox x

Cyberfeed Portal | Apr 26 (3 days ago) | to me

CYBERFEED PORTAL | Cyberfeed Email Digest

ANUBISNETWORKS - LABS

YOU HAVE NEW EVENTS ON YOUR PORTFOLIO

Portfolio's Activity

Last 24 Hours for 25th April

TOTAL ACKNOWLEDGED: **7**

7 events than the previous 24 Hours (for 24th April)

Portfolio's Most Active Infections

Last 24 Hours for 25th April

	OCCURRENCES	VARIATION
	34	17% less
	5	same
	2	same
Nymaim	2	same
NewGOZ	2	100% more

LIVE GLOBE | DASHBOARD

Top Botnet Families Last Hour

- andromeda: 197,797 infections
- ransom: 278,631 infections
- darkbot: 326,503 infections
- sality: 351,505 infections
- conficker_b: 427,123 infections

South America Top Infections Origins

South America Top Countries infected All botnets

- Brazil
- Venezuela
- Argentina
- Chile
- Peru
- Colombia
- Bolivia
- Ecuador
- Uruguay
- Paraguay

All Botnets Infections Over Last day In South America

Top Cleaned Over Time In South America

All Infections In The Last Hour

DOWNLOAD REPORTS

Cyberfeed - Inteligência

Infection detection

- Detection of infected systems communicating with Command & Control servers
- Metadata from real-time communications between machines compromised and C&C servers

Compromised systems

- Malware analysis of files and websites
- Correlation between infected systems (file, email, web) and infection campaigns

Social awareness

- Detection of sensitive information leaked in open social media platforms
- Monitoring of live posts in social websites in open and dark web

Email ecosystem

- Identification of messages being flagged as SPAM and brand abuse campaigns
- Information about URI shortener services, with shortened URI translation
- IP Reputation for an IP Address or domain

Tecnologias Focadas

- **Malware Campaigns**
- **Forensics**
- **Scope global**

Respostas Direcionadas

Situational Awareness & Response

Confiança

- **Real-time**
- **Accuracy**
- **Monitoring**
- **Reporting**
- **Incident Handling**

Backup Slides

