

A red fox with a white chest and tail tip, standing and looking to the right. The fox is positioned on the left side of the slide, partially overlapping the title text.

# The beginner's guide to Threat Intelligence

**Ialle Teixeira**  
Reverse Engineering/Malwares/C++

# #whoami

## Ialle Teixeira

Exploit Database Security Papers @author=9833

Linkedin @isDebuggerPresent

Twitter @DbgShell

Reverse Engineering

Threat Intelligence

Malwares



# AGENDA

- **Introduction**
  - Intelligence Foundations - Foundations and Lifecycle
  - Operational Threat Intelligence
- **Strategic Threat Intelligence**
  - Threat Intelligence Platform
- **Threat Intelligence - NIST Guides**
- **Tactical Threat Intelligence Requirements**
  - Using Open Source Intelligence
  - Free Resources

**The challenges of today's world**

# Intelligence Foundations - Foundations and Lifecycle





# Tactical Threat Intelligence Requirements (NIST Guides)

**NIST Special Publication 800-150**

## Guide to Cyber Threat Information Sharing

Chris Johnson  
Lee Badger  
David Waltermire  
Julie Snyder  
Clem Skorupka

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-150>

**Table 3-3: Traffic Light Protocol, Version 1.0**

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

# • Threat Intelligence Platform



- **Threat Intelligence Sharing/Resources**

The screenshot shows the Censys web interface for searching IPv4 hosts. The top navigation bar includes the Censys logo, a search input field containing "IPV4 Hosts", and a button labeled "uol.com.br". Below the header, there are tabs for "Results" and "Related".

### Quick Filters

For all fields, see [Data Definitions](#)

#### Autonomous System:

- 506 BMEAS-A00001 - BENCHMARK INTERNET GROUP
- 404 Universo Online S.A.
- 44 DIGITALOCEAN-ASN - DigitalOcean, LLC
- 42 AMAZON-AES - Amazon.com, Inc.
- 39 AMAZON-02 - Amazon.com, Inc.

☐ More

### IPv4 Hosts

Page: 1/50 Results: 1,245 Time: 105ms

#### 187.18.60.228

- 🌐 UOL DIVEO S.A. (21911) 📍 Brazil
- 🔗 443/https, 80/http
- 🚫 403 Forbidden 🔒 psec01.uol.com.br, 30anosdeaxe.atarde.uol.com.br, aniversario.uol.com.br
- 🔗 443.https.tls.certificate.parsed.extensions.subject\_alt\_name.dns\_names: aniversario.uol.com.br

#### 200.98.2.94 (manualdaquimica.com)

- 🌐 UOL DIVEO S.A. (19089) 📍 Brazil
- 🔗 443/https, 80/http
- 🚫 403 Forbidden 🔒 psec01.uol.com.br, 30anosdeaxe.atarde.uol.com.br, aniversario.uol.com.br
- 🔗 443.https.tls.certificate.parsed.extensions.subject\_alt\_name.dns\_names: aniversario.uol.com.br

### Protocol:

1,185	80/http
551	25/smtp
517	443/https
123	22/ssh
59	21/ftp

[illegible]

**Verizon**

Summary

Domains

- Current DNS
- DNS History
- Subdomains: 2,189
- Reverse DNS: 5,862
- VHos

IP Addresses

- IP Blocks: 863

Certificates

- Certificates: 21,348

Associations

- Associated Domains: 1,336

Total Subdomains: 2,189

### Summary by Hosting Company

Company	Count
MCI Communications Services, Inc. d/b/a Verizon Business	306
Verizon Data Services LLC	237
Celco Partnership DBA Verizon Wireless	142
Amazon.com, Inc.	110
Advanced Networks & Services Inc.	65

1,337 Total

### Summary by IP

IP Address	Count
93.184.215.233 MCI Communications Services, Inc. d/b/a Verizon Business	17
192.16.31.85 MCI Communications Services, Inc. d/b/a Verizon Business	17
192.16.31.128 MCI Communications Services, Inc. d/b/a Verizon Business	17
192.16.31.89 MCI Communications Services, Inc. d/b/a Verizon Business	16
192.16.31.23 MCI Communications Services, Inc. d/b/a Verizon Business	15

171 Total

Show more [5]

Filter by keyword

1 - 100 of 2,189 results

#	Subdomains	IP	Hosting	Open Ports
1	10-118-0-175-blk.verizon.com *	-	-	-
2	10-118-25-203-blk.verizon.com *	-	-	-

Network Indicators

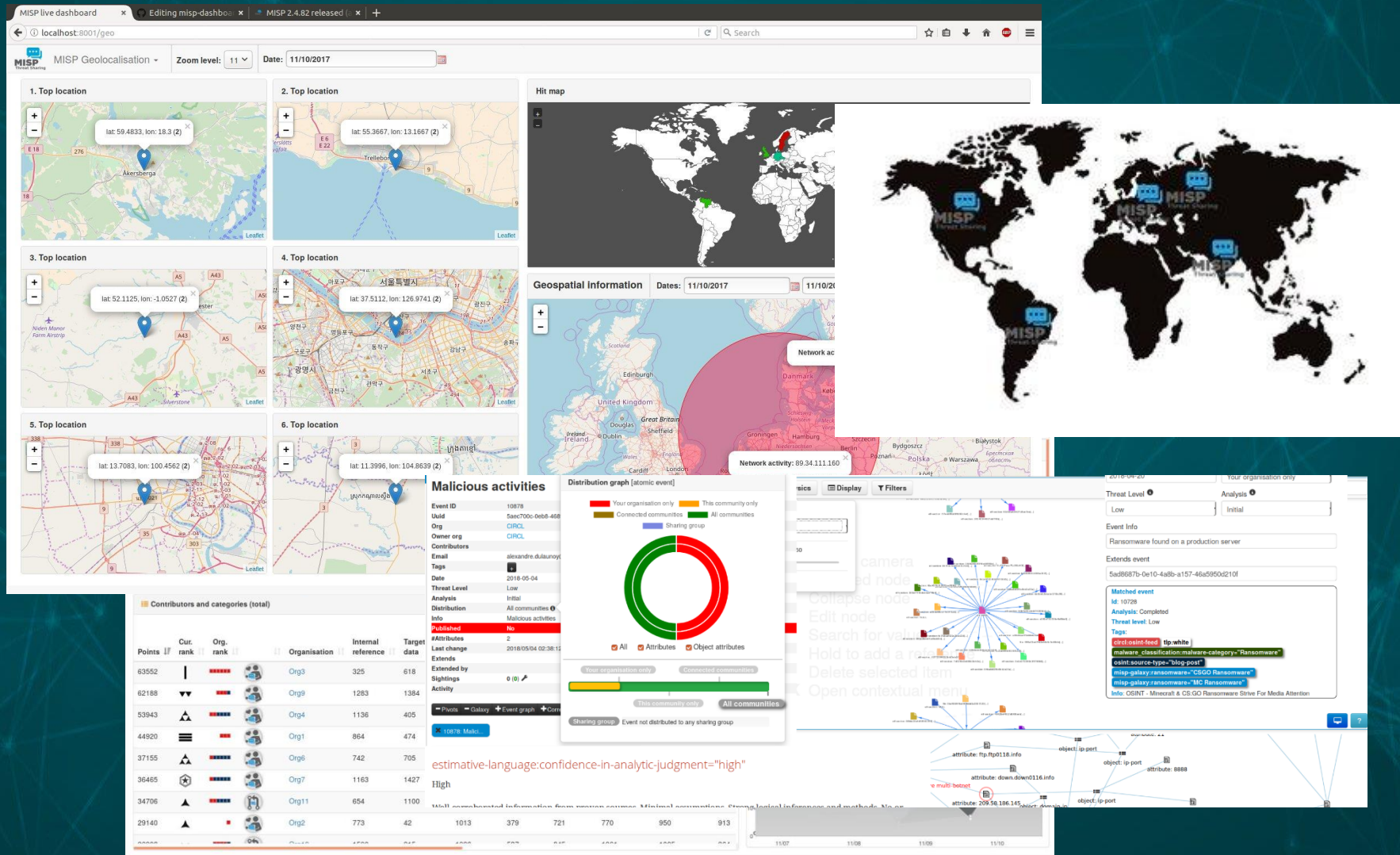
Host	Port	Category	Description
104.28.9.245	80	A Network Trojan was detected	LokBot User-Agent (CharonInferno)
104.28.9.245	80	A Network Trojan was detected	LokBot Request for C2 Commands Detected M1
145.14.14	80	Potential Corporate Privacy	Outdated Flash Version M1
68.89.000	5357	Generic Protocol Command	SURICATA HTTP Host header invalid
46.4.194.4	80	A Network Trojan was detected	ET MALWARE Suspicious User Agent (Autopspider)

EXE files with PDF icons

File Name	Size	Last Seen	Submissions	MITM
2dd8fd441ce2909daae2e9b6f	272.5 KB	2019-04-12 08:37:58 first seen 2019-05-01 10:24:04 last seen	2 submissions 2 mitmatters	EXE
2548f7191f88ddfc7129557d2b0	193.5 KB	2019-04-13 01:56:49 first seen 2019-05-01 10:19:37 last seen	2 submissions 2 mitmatters	PDF
80008be9d1d8c4cadfb74d6e	238 KB	2019-04-12 01:49:37 first seen 2019-05-01 09:47:24 last seen	2 submissions 2 mitmatters	PDF



# Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing





# The challenges of today's world



**Questions?!**

**Questions?!?**

**Questions?!?!**

