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**

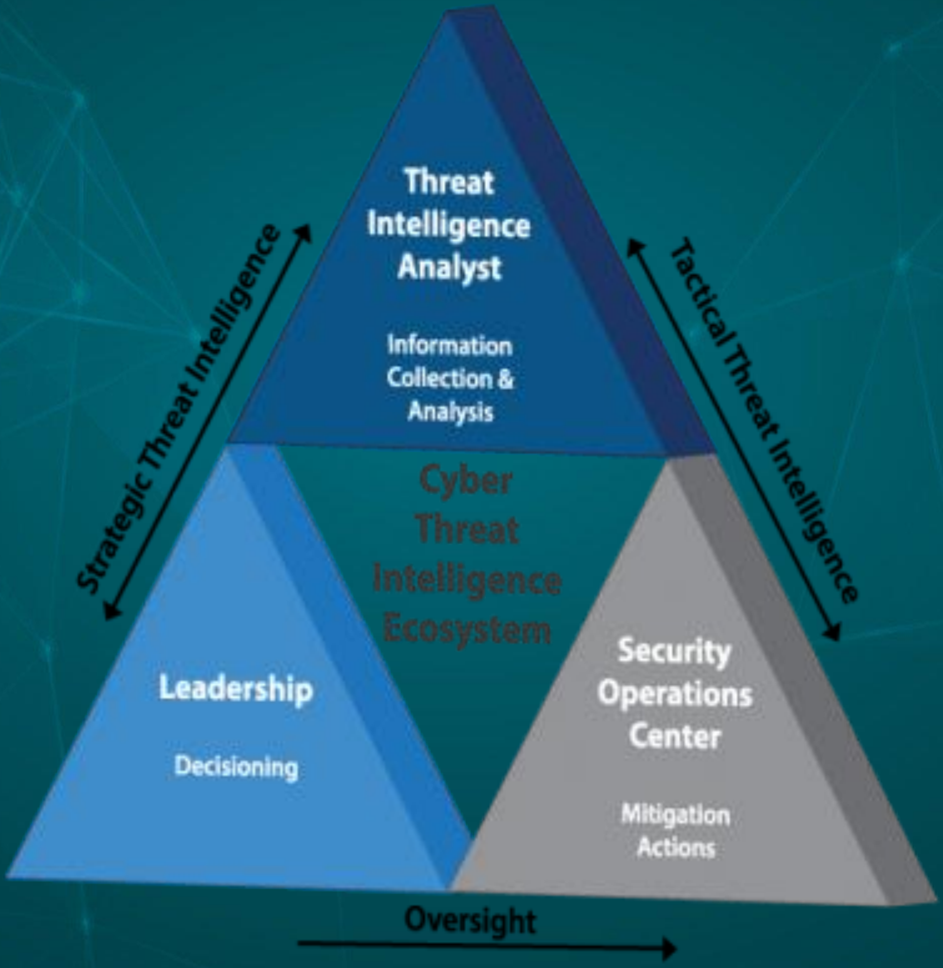
- **Strategic Threat Intelligence**
  - Threat Intelligence Platform

- **Threat Intelligence - NIST Guides**

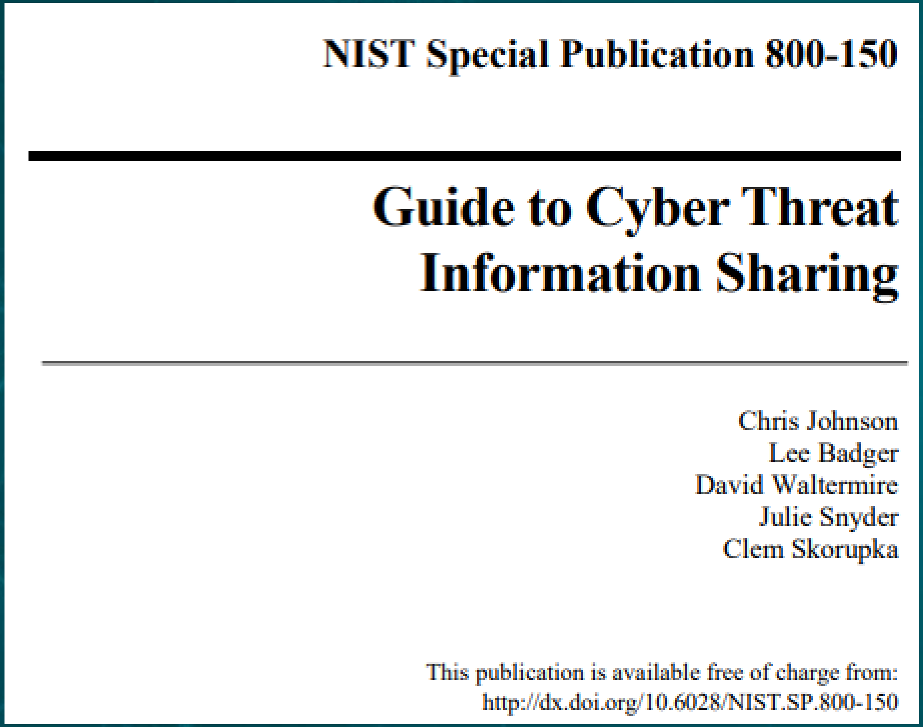
- **Tactical Threat Intelligence Requirements**
  - Using Open Source Intelligence
  - Free Resources

The challenges of today’s world

Intelligence Foundations - Foundations and Lifecycle


Threat Intelligence Analyst
Information Collection & Analysis
Cyber Threat Intelligence Ecosystem
Leadership
Decisioning
Security Operations Center
Mitigation Actions
Strategic Threat Intelligence
Tactical Threat Intelligence
Oversight

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

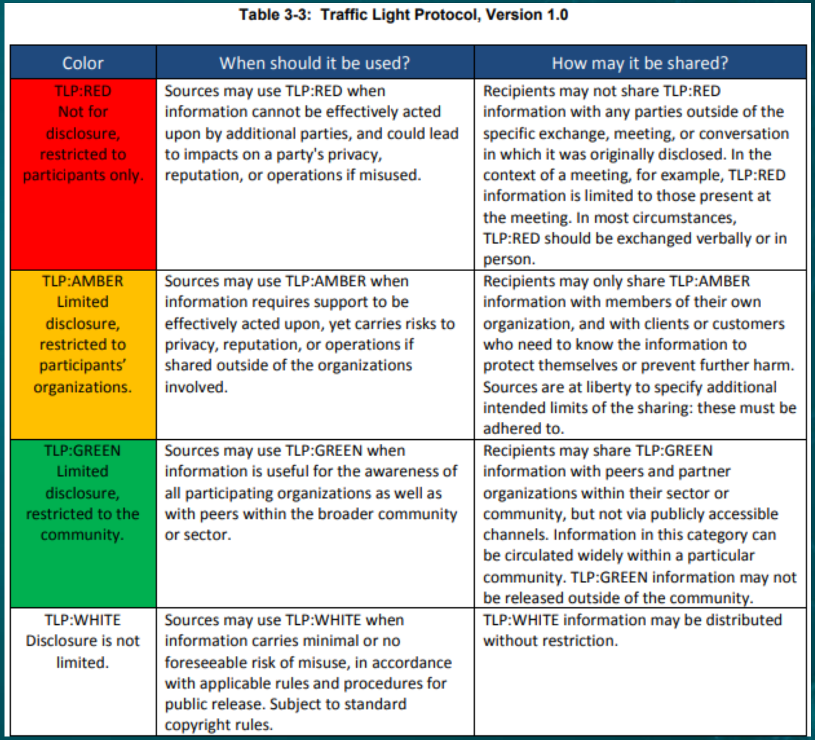
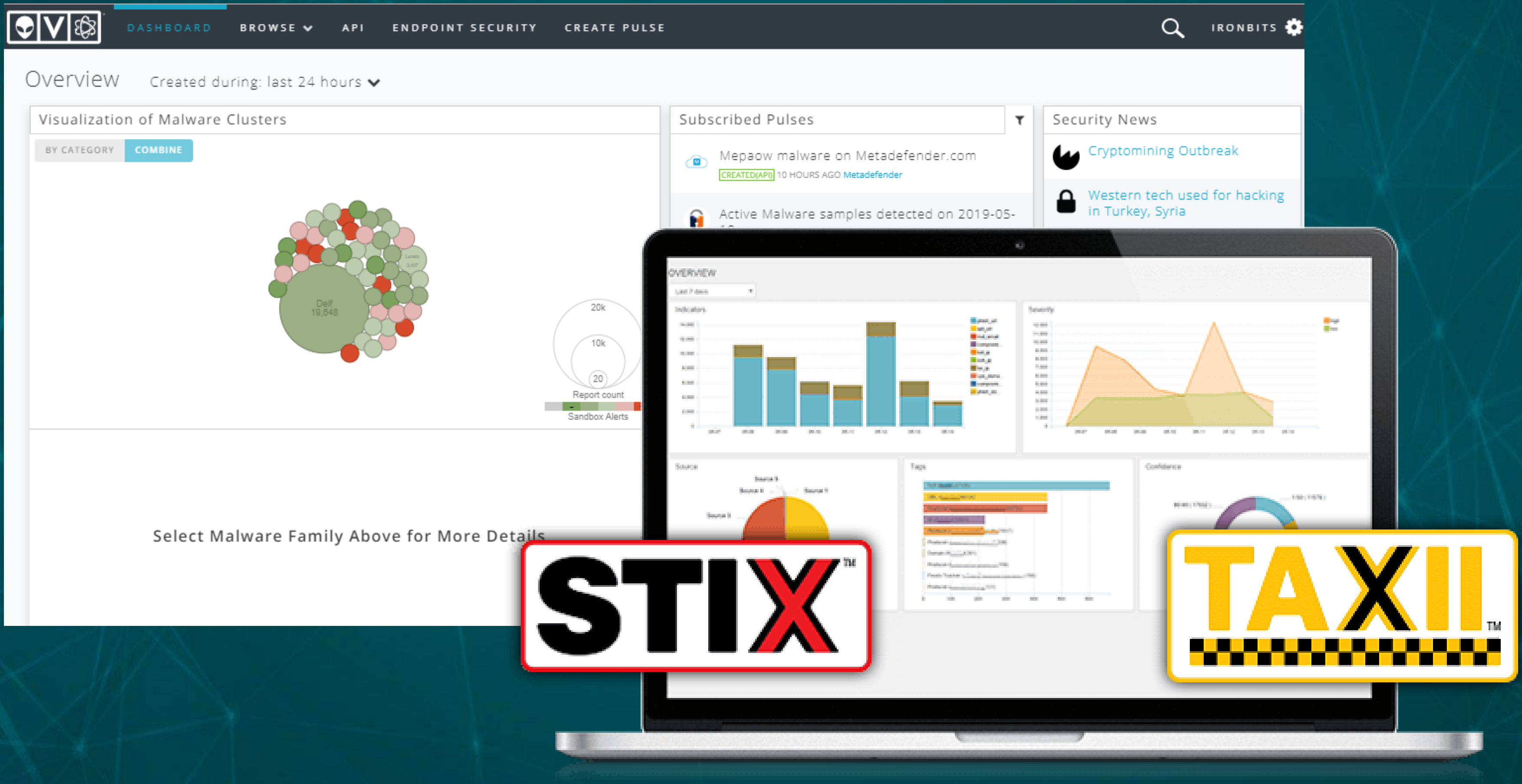


Table 3-3: Traffic Light Protocol, Version 1.0

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.

National Institute of Standards and Technology
U.S. Department of Commerce

- Threat Intelligence Platform



Overview Created during: last 24 hours

Visualization of Malware Clusters

Select Malware Family Above for More Details

Subscribed Pulses

Mepaow malware on Metadefender.com
CREATED(API) 10 HOURS AGO Metadefender

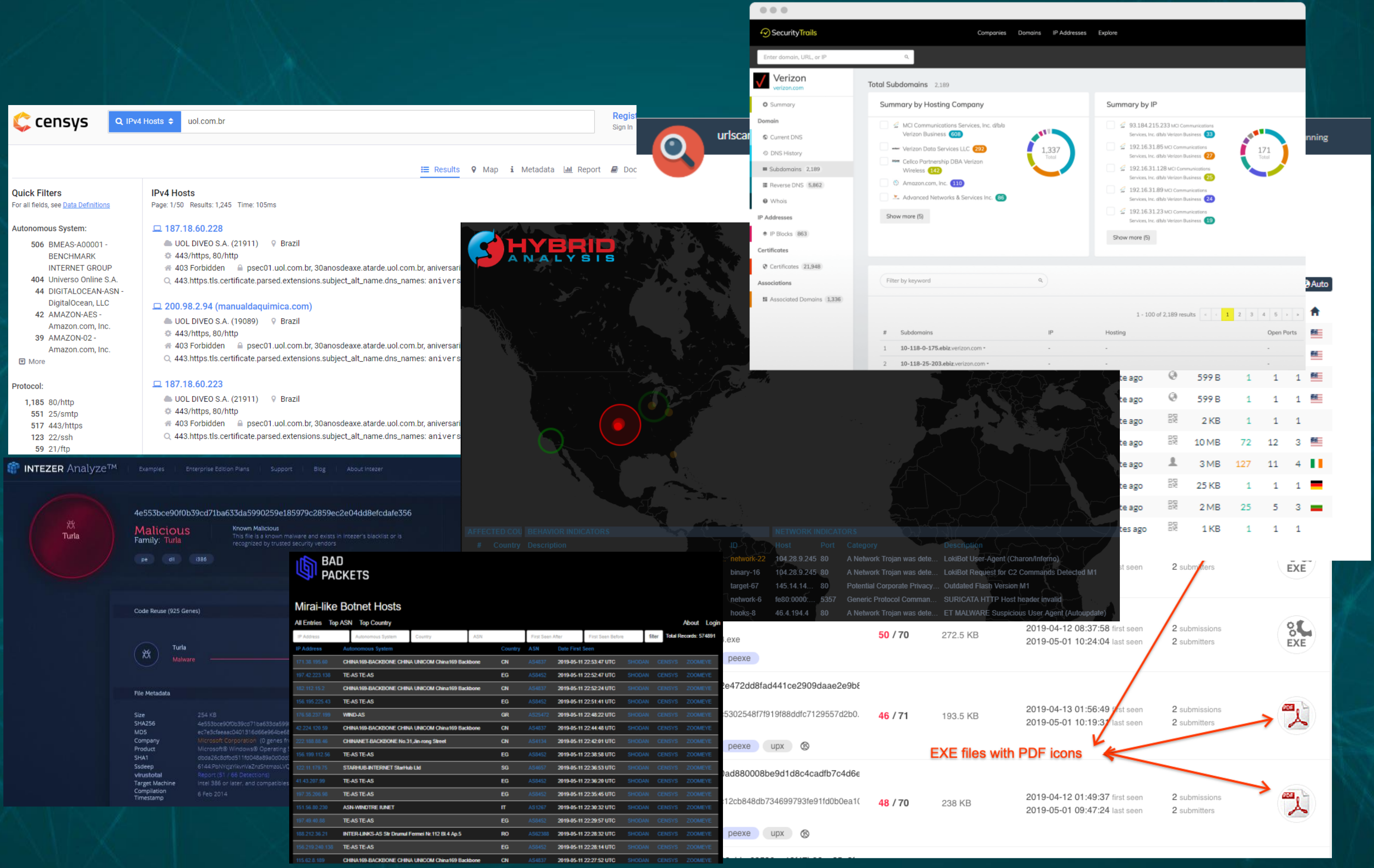
Active Malware samples detected on 2019-05-

Security News

Cryptomining Outbreak

Western tech used for hacking in Turkey, Syria

- # Threat Intelligence Sharing/Resources



censys | IPv4 Hosts | uol.com.br | Register | Sign In

Results | Map | Metadata | Report | Doc

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

Protocol:

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

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, aniversari
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: anivers

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, aniversari
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: anivers

187.18.60.223
UOL DIVEO S.A. (21911) Brazil
443/https, 80/http
403 Forbidden psec01.uol.com.br, 30anosdeaxe.atarde.uol.com.br, aniversari
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names: anivers

urlscan ... nning

SecurityTrails | Companies | Domains | IP Addresses | Explore

Enter domain, URL, or IP

Verizon
verizon.com

Summary
Domain
Current DNS
DNS History
Subdomains 2,189
Reverse DNS 5,862
Whois
IP Addresses
IP Blocks 863
Certificates
Certificates 21,948
Associations
Associated Domains 1,336

Total Subdomains 2,189

Summary by Hosting Company

MCI Communications Services, Inc. d/b/a Verizon Business	608
Verizon Data Services LLC	292
Cellco Partnership DBA Verizon Wireless	142
Amazon.com, Inc.	110
Advanced Networks & Services Inc.	86

1,337 Total

Show more (5)

Summary by IP

93.184.215.233 MCI Communications Services, Inc. d/b/a Verizon Business	33
192.16.31.85 MCI Communications Services, Inc. d/b/a Verizon Business	27
192.16.31.128 MCI Communications Services, Inc. d/b/a Verizon Business	25
192.16.31.89 MCI Communications Services, Inc. d/b/a Verizon Business	24
192.16.31.23 MCI Communications Services, Inc. d/b/a Verizon Business	19

171 Total

Show more (5)

Filter by keyword

1 - 100 of 2,189 results | 1 2 3 4 5

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

Auto

te ago	599 B	1	1	1	🇺🇸
te ago	599 B	1	1	1	🇺🇸
te ago	2 KB	1	1	1	
te ago	10 MB	72	12	3	🇺🇸
te ago	3 MB	127	11	4	🇮🇪
te ago	25 KB	1	1	1	🇩🇪
te ago	2 MB	25	5	3	🇧🇬
tes ago	1 KB	1	1	1	

HYBRID ANALYSIS

AFFECTED COU | BEHAVIOR INDICATORS
# Country Description

NETWORK INDICATORS

ID	Host	Port	Category	Description
network-22	104.28.9.245	80	A Network Trojan was dete...	LokiBot User-Agent (Charon/Inferno)
binary-16	104.28.9.245	80	A Network Trojan was dete...	LokiBot Request for C2 Commands Detected M1
target-67	145.14.14...	80	Potential Corporate Privacy...	Outdated Flash Version M1
network-6	fe80:0000:...	5357	Generic Protocol Comman...	SURICATA HTTP Host header invalid
hooks-8	46.4.194.4	80	A Network Trojan was dete...	ET MALWARE Suspicious User Agent (Autoupdate)

INTEZER Analyze™ | Examples | Enterprise Edition Plans | Support | Blog | About Intezer

Turla

4e553bce90f0b39cd71ba633da5990259e185979c2859ec2e04dd8efcdafe356

Malicious
Family: Turla

Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors

pe | dll | i386

Code Reuse (925 Genes)

Turla
Malware

File Metadata

Size	254 KB
SHA256	4e553bce90f0b39cd71ba633da599
MD5	ec7e3cfaeaac0401316d66e964be68
Company	Microsoft Corporation (0 genes fr
Product	Microsoft® Windows® Operating
SHA1	dbda26c8dfbd511fd048a89a0d0dd
Ssdeep	6144:PbNYcjzYikvnVaZnzShtmzoLVQ
virustotal	Report (51 / 66 Detections)
Target Machine	Intel 386 or later, and compatibles
Compilation Timestamp	6 Feb 2014

BAD PACKETS

Mirai-like Botnet Hosts

All Entries | Top ASN | Top Country | About | Login

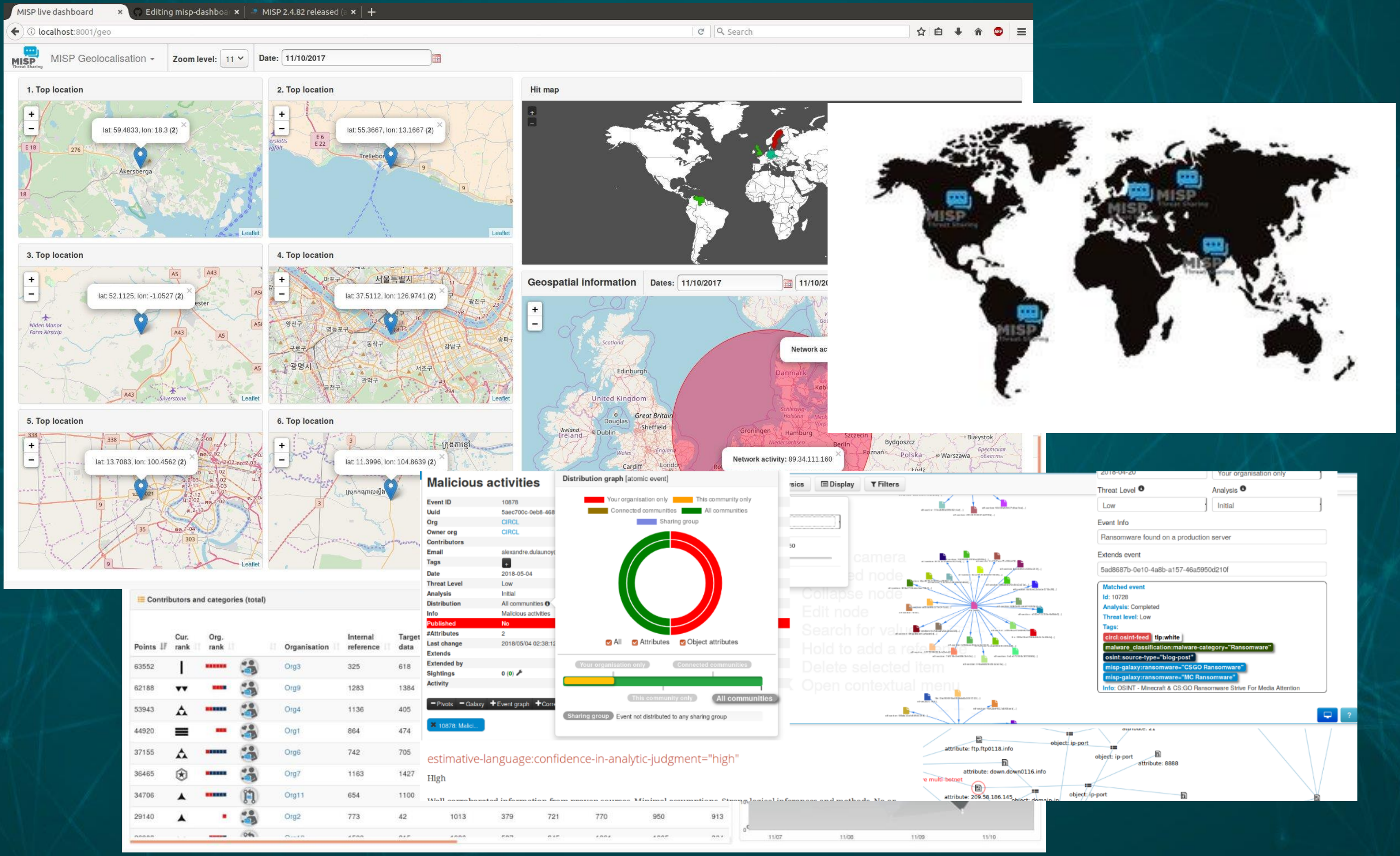
IP Address | Autonomous System | Country | ASN | First Seen After | First Seen Before | filter | Total Records: 574891

IP Address	Autonomous System	Country	ASN	Date First Seen			
171.38.195.60	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	CN	AS4837	2019-05-11 22:53:47 UTC	SHODAN	CENSYS	ZOOMEYE
197.42.223.138	TE-AS TE-AS	EG	AS8452	2019-05-11 22:52:47 UTC	SHODAN	CENSYS	ZOOMEYE
182.112.15.2	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	CN	AS4837	2019-05-11 22:52:24 UTC	SHODAN	CENSYS	ZOOMEYE
156.195.225.43	TE-AS TE-AS	EG	AS8452	2019-05-11 22:51:41 UTC	SHODAN	CENSYS	ZOOMEYE
176.58.237.199	WIND-AS	GR	AS25472	2019-05-11 22:48:22 UTC	SHODAN	CENSYS	ZOOMEYE
42.224.120.59	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	CN	AS4837	2019-05-11 22:44:48 UTC	SHODAN	CENSYS	ZOOMEYE
222.188.88.46	CHINANET-BACKBONE No.31,Jin-rong Street	CN	AS4134	2019-05-11 22:42:01 UTC	SHODAN	CENSYS	ZOOMEYE
156.199.112.56	TE-AS TE-AS	EG	AS8452	2019-05-11 22:38:58 UTC	SHODAN	CENSYS	ZOOMEYE
122.11.179.75	STARHUB-INTERNET StarHub Ltd	SG	AS4657	2019-05-11 22:36:53 UTC	SHODAN	CENSYS	ZOOMEYE
41.43.207.99	TE-AS TE-AS	EG	AS8452	2019-05-11 22:36:20 UTC	SHODAN	CENSYS	ZOOMEYE
197.35.206.98	TE-AS TE-AS	EG	AS8452	2019-05-11 22:35:45 UTC	SHODAN	CENSYS	ZOOMEYE
151.56.80.230	ASN-WINDTRE IUNET	IT	AS1267	2019-05-11 22:30:32 UTC	SHODAN	CENSYS	ZOOMEYE
197.49.40.88	TE-AS TE-AS	EG	AS8452	2019-05-11 22:29:57 UTC	SHODAN	CENSYS	ZOOMEYE
188.212.36.21	INTER-LINKS-AS Str Drumul Fermei Nr.112 Bl.4 Ap.5	RO	AS62388	2019-05-11 22:28:32 UTC	SHODAN	CENSYS	ZOOMEYE
156.219.240.138	TE-AS TE-AS	EG	AS8452	2019-05-11 22:28:14 UTC	SHODAN	CENSYS	ZOOMEYE
115.62.8.189	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	CN	AS4837	2019-05-11 22:27:52 UTC	SHODAN	CENSYS	ZOOMEYE

.exe peexe	50 / 70	272.5 KB	2019-04-12 08:37:58 first seen 2019-05-01 10:24:04 last seen	2 submissions 2 submitters	EXE
2e472dd8fad441ce2909daae2e9b8 5302548f7f919f88ddfc7129557d2b0. peexe upx	46 / 71	193.5 KB	2019-04-13 01:56:49 first seen 2019-05-01 10:19:37 last seen	2 submissions 2 submitters	
0ad880008be9d1d8c4cadfb7c4d6e 12cb848db734699793fe91fd0b0ea1(peexe upx	48 / 70	238 KB	2019-04-12 01:49:37 first seen 2019-05-01 09:47:24 last seen	2 submissions 2 submitters	

EXE files with PDF icons

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



Malicious activities

Event ID	10878
Uuid	5aec700c-0eb8-468
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy
Tags	+
Date	2018-05-04
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	Malicious activities
Published	No
#Attributes	2
Last change	2018/05/04 02:38:12
Extends	
Extended by	
Sightings	0 (0)
Activity	

Distribution graph [atomic event]

Sharing group: Event not distributed to any sharing group

estimative-language:confidence-in-analytic-judgment="high"

High

Well corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No or

Contributors and categories (total)

Points	Cur. rank	Org. rank		Organisation	Internal reference	Target data						
63552				Org3	325	618						
62188				Org9	1283	1384						
53943				Org4	1136	405						
44920				Org1	864	474						
37155				Org6	742	705						
36465				Org7	1163	1427						
34706				Org11	654	1100						
29140				Org2	773	42	1013	379	721	770	950	913

Your organisation only

Threat Level: Low

Analysis: Initial

Event Info: Ransomware found on a production server

Extends event: 5ad8687b-0e10-4a8b-a157-46a5950d210f

Matched event
Id: 10728
Analysis: Completed
Threat level: Low
Tags:
circl:osint-feed
tlp:white
malware_classification:malware-category="Ransomware"
osint:source-type="blog-post"
misp-galaxy:ransomware="CSGO Ransomware"
misp-galaxy:ransomware="MC Ransomware"
Info: OSINT - Minecraft & CS:GO Ransomware Strive For Media Attention

The challenges of today’s world

“Information is a source of learning. But unless it is organized, processed, and available to the right people in a format for decision making, it is a burden, not a benefit.” **William G. Pollard**

Resources:

- Cyber Threat Intelligence Support to Incident Handling

  https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/38150
- HIPAA 2015-Threat Intelligence for Dummies

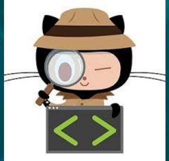
  https://csrc.nist.gov/Presentations/2015/HIPAA-2015-Threat-Intelligence-for-Dummies
- CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING

  https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=923332
- Guide to Cyber Threat Information Sharing

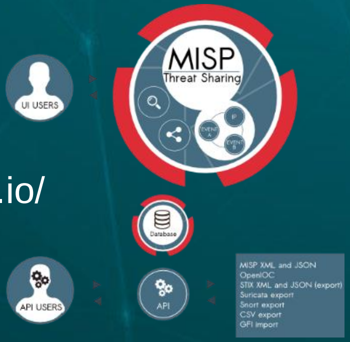
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
- *MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*

  https://www.misp-project.org

A curated list of Awesome Threat Intelligence resources:
https://github.com/hslatman/awesome-threat-intelligence



https://oasis-open.github.io/



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

STIX/TAXII feed
https://www.anomali.com/community
Sharing threat intelligence just got a lot easier!

Questions?!

Questions?!?

Questions?!?!