Sharing Threat Indicators and Security Ranking, an opportunity for the Internet Community.

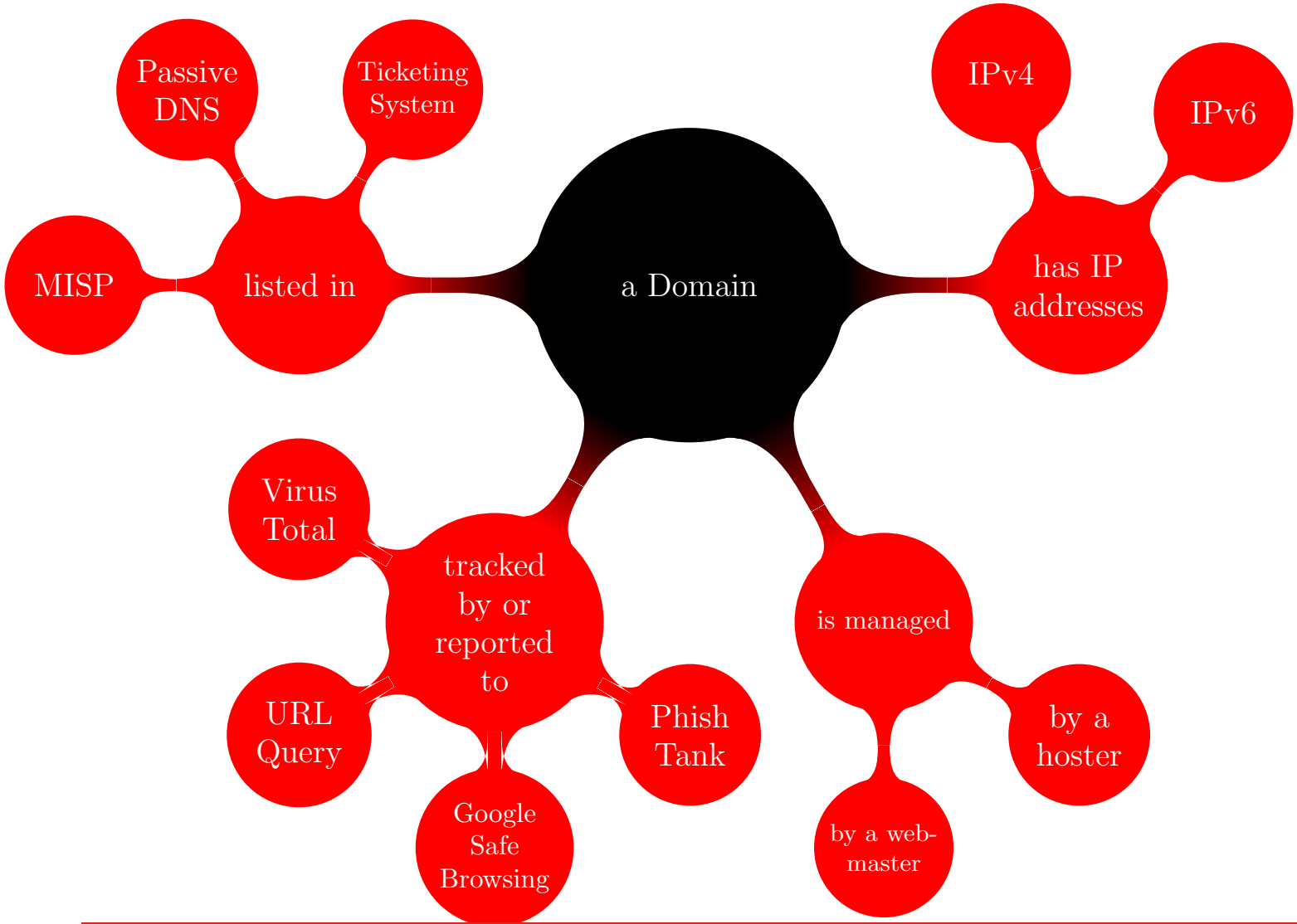
How to Track Suspicious Resources on Internet without Losing your Time and your Mind

CIRCL
Computer Incident
Response Center
Luxembourg

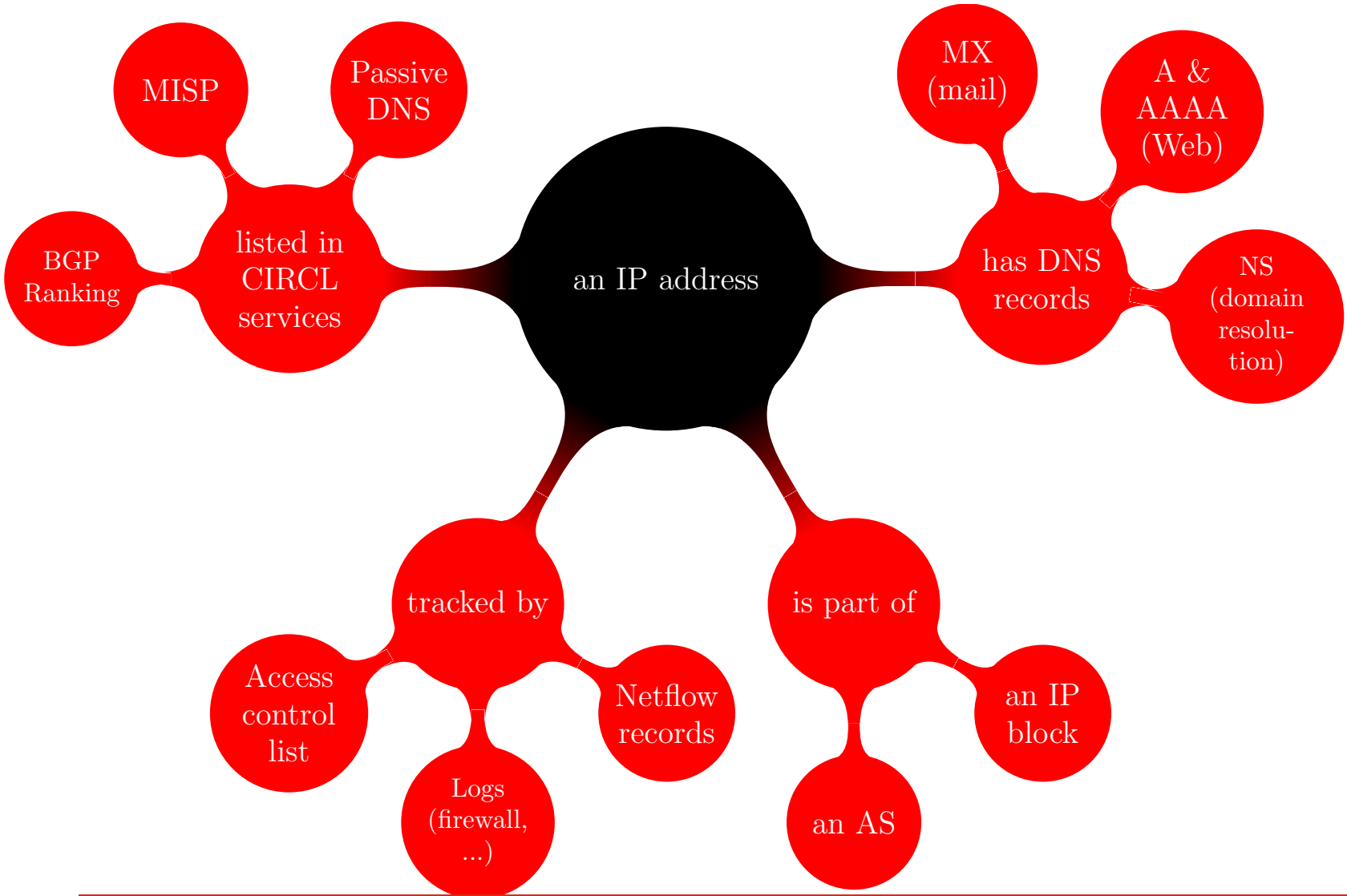
Raphaël Vinot

November 18, 2014

Internet Resources and Security



Internet Resources and Security



The proliferation of information - challenges

- Require fast lookup and simple tools and APIs
- Corelation of information
- Datamining
- Time-based events
- Contacts points

BGP Ranking - metrics on providers

- Correlation of a large variety of private/public datasets including IP, prefixes or ASN for suspicious activities.
- **Allow to provide telemetrics about internet providers worldwide**
- Lookup by AS Number
- Lookup by IP Address
- Years of history
- API to query the service automatically
- `http://bgpranking.circl.lu/index`

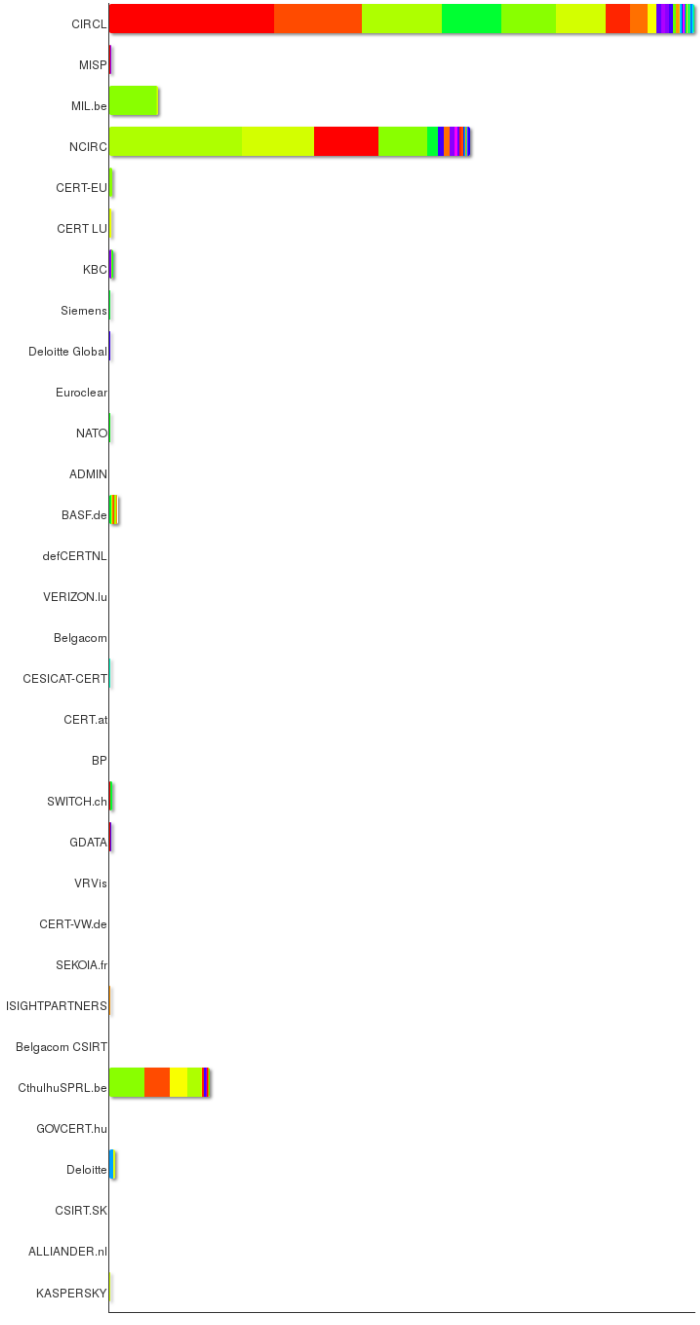
BGP Ranking

There is **14720** entries in the list of asns with malicious content. The top 100 is printed on this page.

ASN	Description	Rank	Source(s)
64097	No ASN description has been found.	1.89078125	Alienvault, SshblBase, DshieldDaily, EmergingThreatsCompromized, BlocklistDeSsh
198540	ELAN-AS Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz. Andrzej Niechcial,PL	1.49328125	BlocklistDeApache, Alienvault, BlocklistDeMail, CleanMXMalwares, BlocklistDeStrong, CleanMXPortals, DshieldDaily, BlocklistDeBots
49934	VVPN-AS PE Voronov Evgen Sergiyovich,UA	1.355703125	BlocklistDeApache, Alienvault, DshieldTopIPs, SshblBase, DshieldDaily, EmergingThreatsCompromized, BlocklistDeSsh, BlocklistDeBots
201781	TELECLICK-AS Unikalnie Technologii ltd.,RU	1.146484375	NothinkHTTP
62403	DISKGROUP Disk Group Ltd.,CZ	1.1196875	Alienvault, DshieldDaily, CleanMXMalwares
47142	STEEPHOST-AS PP Andrey Kiselev,UA	1.11358473558	BlocklistDeApache, Alienvault, NothinkIRC, BlocklistDeStrong, NothinkHTTP, DshieldDaily, BlocklistDeBots
27385	QUALYS - QUALYS, Inc.,US	1.08162109375	Alienvault, SshblBase, DshieldDaily
59564	UNIT-IS-AS Unit-IS Ltd.,UA	1.07978236607	BlocklistDeApache, Alienvault, DshieldTopIPs, Shunlist, DshieldDaily, BlocklistDeStrong, BlocklistDeBots
27176	DATAWAGON - DataWagon LLC,US	1.07878348214	CIArmy, BlocklistDeImap, Alienvault, DshieldTopIPs, BlocklistDeMail, SshblBase, ZeustrackerIpBlockList, DshieldDaily

Malware information sharing platform - targeted attacks

- More than 50 trusted partners from all over the world
- More than 60.000 indicators (IPs, domains, file hashes, samples...)
- More than 600 events seen by a large variety of organisations
- Create automatically relations between malware and their attributes, and between different events
- Simple lookup
- Straightforward creation of new events
- API to query the service automatically
- `http://circl.lu/services/misp-malware-information-sharing-platform/`



OSINT - The Uroburos case: new sophisticated RAT identi...

Event ID	655
Uuid	5461eb1f-fa4c-48cb-8512-0c93950d210b
Org	CIRCL
Owner org	CIRCL
Contributors	CthulhuSPRL.be
Email	alexandre.dulaunoy@circl.lu
Tags	Type:OSINT x TLP:GREEN x +
Date	2014-11-11
Threat Level	High
Analysis	Completed
Distribution	All communities
Description	OSINT - The Uroburos case: new sophisticated RAT identified Agent.BTZ's successor, ComRAT,
Published	Yes

Related Events

2014-11-13 (665) 2014-11-04 (639) 2014-08-18 (526)
2014-08-07 (510) 2014-08-07 (514) 2014-06-13 (471)
2014-06-06 (571) 2014-05-14 (373) 2014-03-10 (6)
2014-03-03 (356) 2014-02-28 (14) 2009-11-01 (415)

Pivots | Attributes | Discussion

655: OSINT ...

Date	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2014-11-11	Antivirus detection	text	ComRAT			No	All communities	
2014-11-11	Antivirus detection	text	Agent.BTZ		6	No	All communities	
2014-11-11	Antivirus detection	text	Turla.E			No	All communities	
2014-11-11	Payload installation	md5	51e7e58a1e654b6e586fe36e10c67a73			Yes	All communities	
2014-11-11	Payload installation	md5	e6ce1f962a47479a86ff2e67129f4ecc			Yes	All communities	
2014-11-11	Payload installation	md5	ec7e3cfaeaac0401316d66e964be684e			Yes	All communities	
2014-11-11	Payload installation	md5	0ae421691579ff6b27f65f49e79e88f6		639	Yes	All communities	
2014-11-11	Payload installation	md5	255118ac14a9e66124f7110acd16f2cd		639	Yes	All communities	
2014-11-11	Payload installation	md5	b407b6e5b4046da226d6e189a67f62ca		639	Yes	All communities	
2014-11-11	Payload installation	md5	8ebf7f768d7214f99905c99b6f8242dc			Yes	All communities	
2014-11-11	Payload installation	md5	9d481769de63789d571805009cbf709a			Yes	All communities	
2014-11-11	Payload installation	md5	83a48760e92bf30961b4a943d3095b0a			Yes	All communities	
2014-11-11	Payload installation	md5	ea23d67e41d1f0a7f7e7a8b59e7cb60f		639	Yes	All communities	

Conclusion

- Attackers are often ahead, sharing and communication plays an important role for their success
- If you share threat intel and indicators, you can:
  - Avoid duplicate analysis work and concentrate on the unknown elements of an attack
  - Automate detection in your infrastructure and reduce the incident response time
- Do you want to share IOCs? Help others and benefit? $\rightarrow$ info@circl.lu
- PGP Key: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5