

23 September 2017

BSides Zürich

The Social Networks of the Security Community

Jeroen Massar
jeroen@massar.ch



Jeroen Massar



private:

<https://jeroen.massar.ch> & jeroen@massar.ch

work:

Massar Networking (Independent security & engineering researcher)

funtime:

Secluded.ch / Trident Coder ← hat of the day

Ops-Trust Sysadmin Team

Before sunset: SixXS Staff

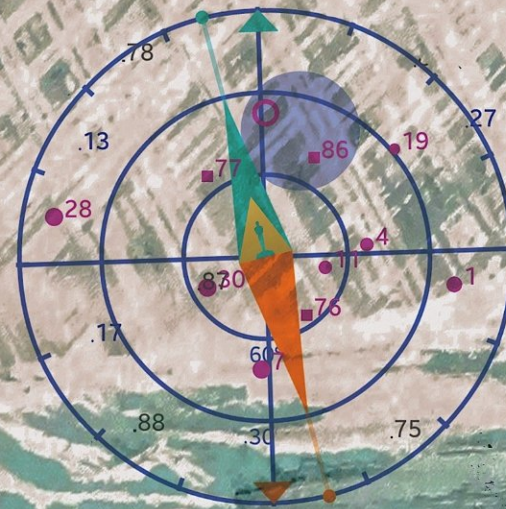
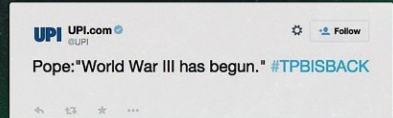
2600



Volume Thirty-Two, Number One!
DIGITAL EDITION Spring 2015

2600

The Hacker Quarterly



Latitude
78.252785N

Longitude
15.409617E

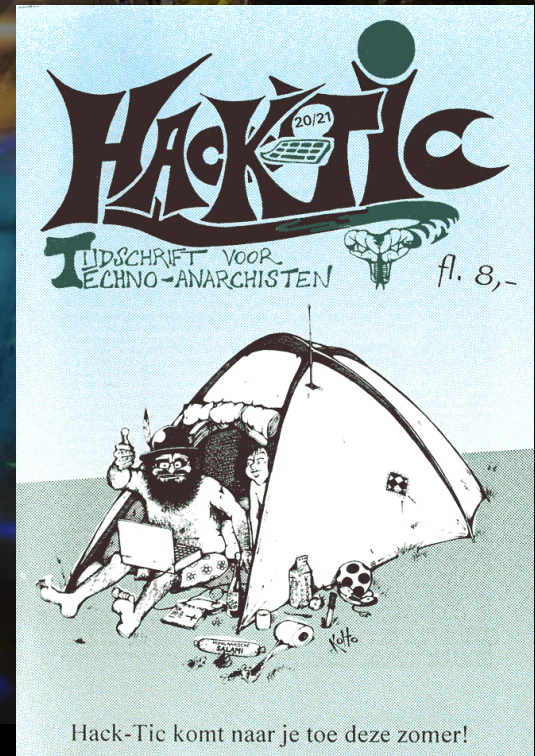


Hacktic

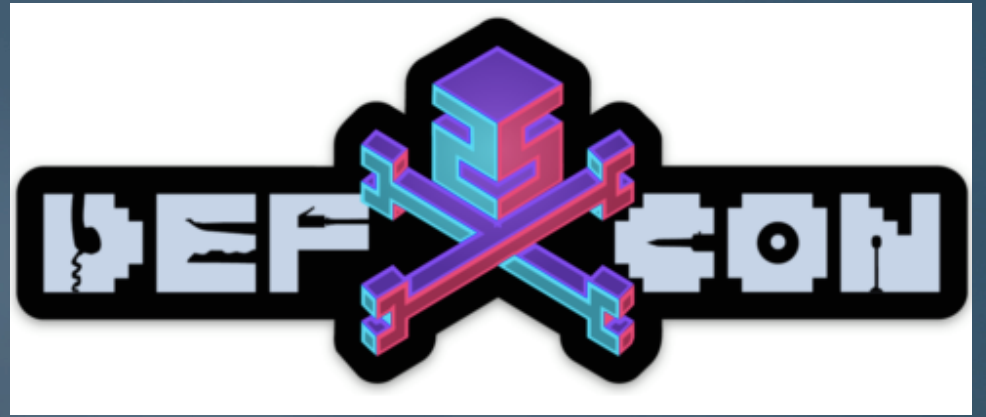
- 1989 - Galactic Hacker Party (GHP)
- 1993 - Hacking at the End of the Universe (HEU)
- 1997 - Hacking In Progress (HIP)
- 2001 - Hackers At Large (HAL)
- 2005 - What The Hack (WTH)
- 2009 - Hacking at Random (HAR)
- 2013 - Observe. Hack. Make. (OHM)
- 2017 - Still Hacking Anyway (SHA)



SHA2017







RSA



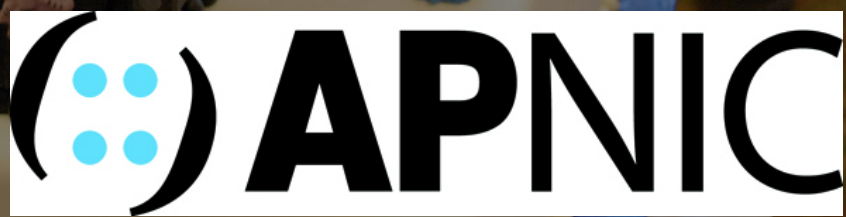


RIPE NCC

RIPE NETWORK COORDINATION CENTRE



American Registry for Internet Numbers





SIGS

**Security Interest
Group Switzerland**



OWASP Switzerland



Information
Security Society
Switzerland



ISSA

Information Systems Security Association



Ops-Trust

OPERATIONS SECURITY TRUST

[Login](#)

Mission

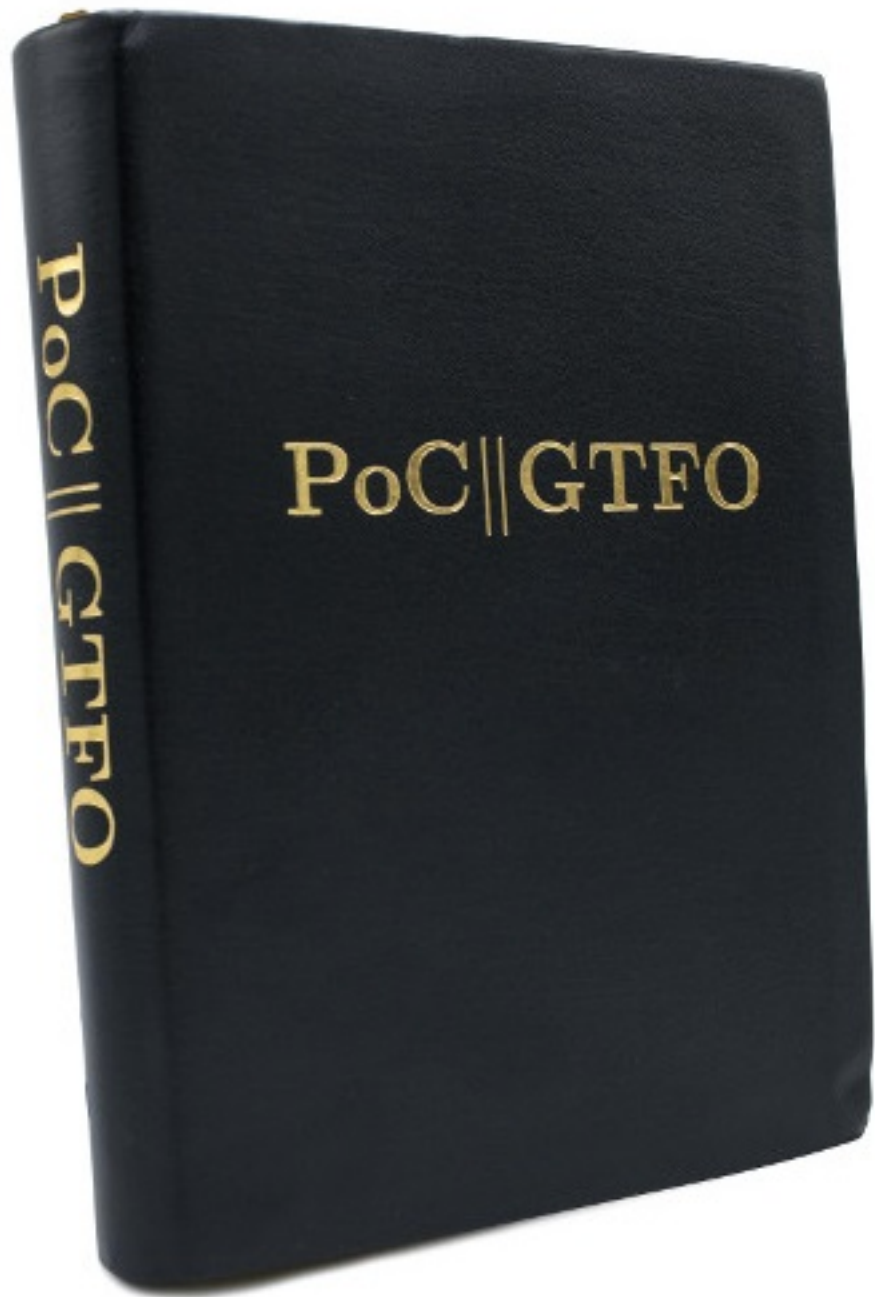
Operations Security Trust (or "Ops-T") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. Ops-T carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:

1. sphere of trust;
2. sphere of action;
3. the ability to maintain a "need to know" confidentiality.

Operations Security Trust (or "Ops-T") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on the malleasant behaviors which threaten the Internet.

Members:

- will be privy to lists of infected IP addresses, compromised accounts, bot c&c lists and other data that should be acted upon.
- are expected to take appropriate action within their domain of control.
- are expected to contribute data as appropriate and in a fashion that does not violate any laws or corporate policies.



PoC || GTFO

PoC || GTFO



BOOSIDES ZURICH



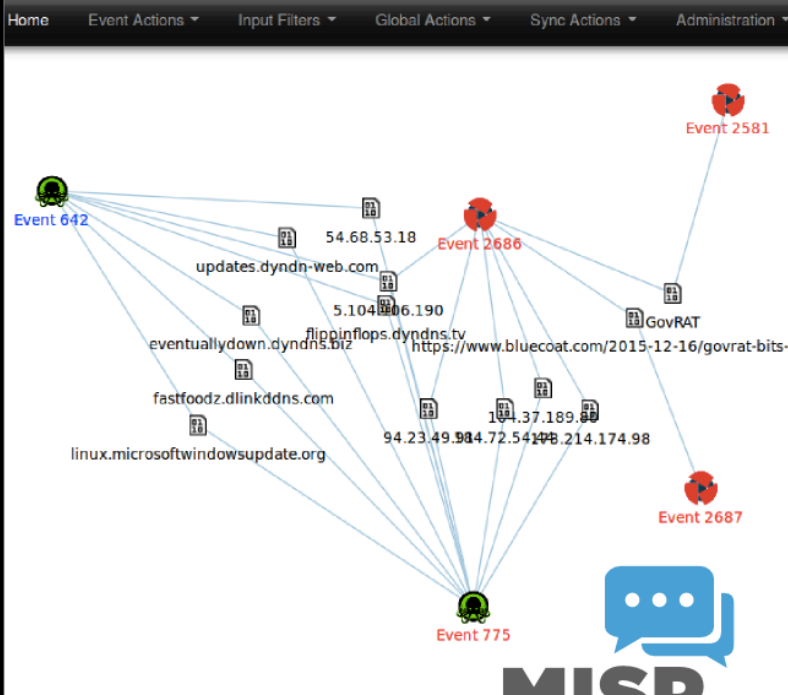
DC4131



AREA 51



SAVE THE DATE
15.-16.JUNE 2018



TLP Taxonomy Library

Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

Navigation: < previous | next >

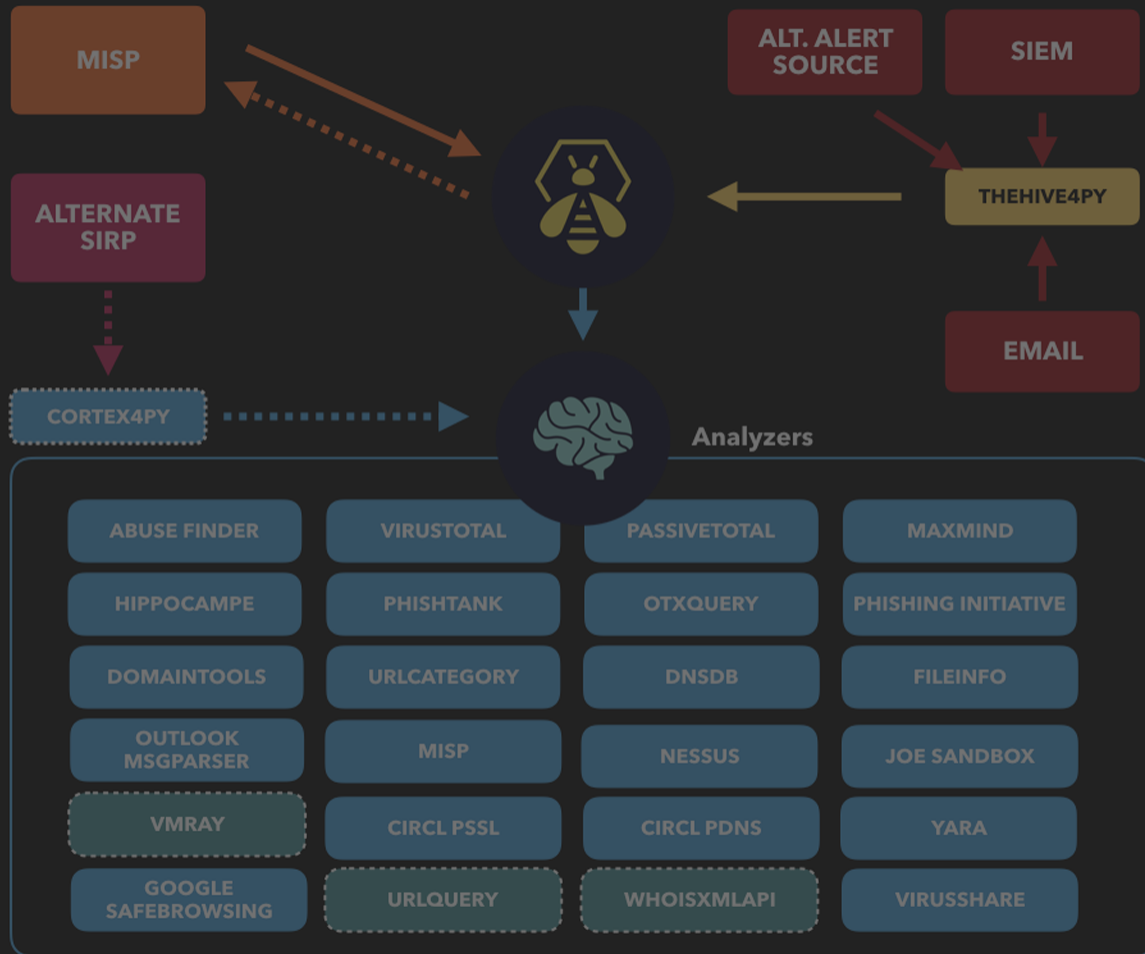
Filter:

Tag	Expanded	Events	Tag	Action
<input type="checkbox"/>	tlp:red (TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
<input type="checkbox"/>	tlp:amber (TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
<input type="checkbox"/>	tlp:green (TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
<input type="checkbox"/>	tlp:white (TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	
<input type="checkbox"/>	tlp:ex:chr (TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	<input checked="" type="checkbox"/>	APT		31	
7	<input checked="" type="checkbox"/>	Actionable:NO		5	
3	<input checked="" type="checkbox"/>	TLP:AMBER	tlp	131	
8	<input checked="" type="checkbox"/>	TLP:EX:CHR	tlp	11	
5	<input checked="" type="checkbox"/>	TLP:GREEN	tlp	550	
4	<input checked="" type="checkbox"/>	TLP:RED	tlp	3	
2	<input checked="" type="checkbox"/>	TLP:WHITE	tlp	531	
10	<input checked="" type="checkbox"/>	TO:HIDE		2	
9	<input checked="" type="checkbox"/>	TODO		9	

Published	Org	Owner Org	Id	Tags	#Attr	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGRNAME	83	tlp:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE FANSMO	All	
✓	CUDESO	ORGRNAME	91	tlp:white	3	admin@admin.test	2016-03-07	Low	Completed	Add Servng Platform Used By PUA Also Delivers Magnitude Exploit Kit	All	
✓	CUDESO	ORGRNAME	82	tlp:white	3	admin@admin.test	2016-03-25	Low	Completed	PETVA Cryptransmission Overwrites MBR to Lock Users Out of Their Computers	All	
✗	CIRCL	ORGRNAME	5	tlp:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turia - Harnessing SSL Certificates Using Infrastructure Chaining	All	
✗	CIRCL	ORGRNAME	43	tlp:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	
✓	CIRCL	ORGRNAME	10	tlp:white	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	
✓	CIRCL	ORGRNAME	44	tlp:white	290	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - AiDroidx (122), Lucky	All	
✓	CIRCL	ORGRNAME	16	tlp:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AcsDeceiver: First iOS Troje Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	
✓	CUDESO	ORGRNAME	71	tlp:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSpiff Malware Used in Macro-based Attacks	All	
✓	CIRCL	ORGRNAME	25	tlp:white	32	admin@admin.test	2016-03-16	Low	Initial	Lucky (2016-03-16) - Ai	All	

TheHive Project



GNU Mailman



Schleuder



<https://schleuder.nadir.org/>

Trident



Sign In

Home Login



Home

Home

Mission

Operations Security Trust (or "Ops-T") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. Ops-T carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:

- * sphere of trust;
- * sphere of action;
- * the ability to maintain a "need to know" confidentiality.

Operations Security Trust (or "Ops-T") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on



Mentoring!

Trust?



Questions?

Jeroen Massar

jeroen@massar.ch

<https://jeroen.massar.ch>

