Network Security Using ntopng



Understanding Host Behaviour [1/2]

- Security attacks can originate from both local and remote hosts.
- It is important to characterise host behaviour in order to detect invalid traffic patterns and thus react.
- Typical misbehaved hosts include:
 - Multiple (low bandwidth) egress connections.
 - Connections with hosts on countries unlikely to be contacted.
 - Use of unfriendly protocols such as SSL connections with self-signed certificates.



Understanding Host Behaviour [2/2]

 Host behaviour is the result of the combination of flow traffic analysis.

SSL Certificate	Client Requested: luca.ntop.org	Server Certificate: shop.ntop.org
Max (Estimated) TCP Throughput	Client -> Server: 91.57 Kbit	Client
TCP Flags	Client -> Server: FIN SYN PUSH ACK	Client - Server: FIN SYN PUSH ACK
	This flow is completed and will expire soon.	
Flow Status	SSL Certificate Mismatch	



IPv6 Address Assignment

- IPv6 hosts can configure themselves automatically using the Neighbour Discovery Protocol in ICMPv6 discovery messages.
- To find out unwanted advertisers do:

ICMPV6

IP Version



Applications T -

10 -

Hosts-

Active ICMPV6 Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info♥
Info	ICMPV6 🖒	IPv6-ICMP		an in the second state (11	< 1 sec	Client	0 bps —	86 B	Neighbor Solicitation
Info	ICMPV6 🖒	IPv6-ICMP	fe80::8aa2:5eff:fee6	ff02::1	1 sec	Client	0 bps —	172 B	Neighbor Advertisement
Info	ICMPV6 🖒	IPv6-ICMP	and the second s	ff02::1	1 min, 10 sec	Client	0 bps —	430 B	Neighbor Advertisement
Info	ICMPV6 🖒	IPv6-ICMP	fe80::f6b5:2f00:fc:a		< 1 sec	Client	0 bps —	78 B	Neighbor Advertisement
Info	ICMPV6 🖒	IPv6-ICMP	fe80::226:88ff:fe7f:	ff02::1	1 min, 10 sec	Client	0 bps —	430 B	Neighbor Advertisement
Info	ICMPV6 🖒	IPv6-ICMP	D	ff02::1	1 sec	Client	0 bps —	172 B	Neighbor Advertisement

Showing 1 to 6 of 6 rows



Detecting Command & Control [1/2]

- In case an <u>internal</u> (external accesses are mediated by firewall devices and thus are more difficult) host is infected, such host can run an Internet robot (a.k.a. bot) for running automatic tasks over the Internet.
- Malicious use of bots is the coordination and operation of an automated attack on networked computers.
- A typical bot behaviour consists of opening (a) several (b) low-bandwidth (c) client connection over unknown layer-7 protocols to instruct remote bots.



Detecting Command & Control [2/2]

	nto	ρ				* ∞ 	Flows Hosts - Devices -	Interfaces 👻 🔅	• U• Q	Search Host			
	Host:		Traffic	Packets	Ports	Peers Protocols	Flows Talkers 🔇 🕍 🏟	5					
Unknown Protocol	Active	e Flows	Sar	me I	Port		Diffe	erent Tar	gets	50 v Applica	tions -	_ittle	Traffic
	2	Application	L4 Proto	VLAN	Client		Server	Duration♥	Actual Thpt	Total Bytes	Info		
	Info	? Unknown	🛕 ТСР	- 10		:50933	90.113.215.107:64963	3 sec	1.31 Kbit 🛧	883 B	BK.		
	Info	? Unknown	🛕 ТСР			:50933	90.62.176.114:50191	3 sec	535.17 bps 🛧	469 B	and the second		
	Info	? Unknow	🗡 🚹 ТСР	1		:50933	181.229.201.186:49719	3 sec	0 bps —	307 B			
Low 🛫	Info	? Unknown	🛕 ТСР	2		:57316	77.144.172.122:http	3 sec	0 bps —	580 B			
Bandwidth	Info	? Unknown				:50933	181.229.201.186:49839	5 sec	637.41 bps 🛧	533 B			
Danamati	Info	? Unknown	🛕 ТСР			:50933	90.0.70.375-50.01.4	2 sec.	0 bps —	262 B			
	Info	? Unknown	🛕 ТСР	100		:57318	77.144.172.122:http	2 sec	0 bps —	580 B			
	Info	? Unknown	🛕 ТСР			:50933	89.159.84.197:52345	< 1 sec	0 bps	64 B			
	Info	? Unknown	🛕 ТСР			:50933	87.91.126.40:50710	2 sec	0 bps	1.27 KB			
	Info	? Unknown	🛕 ТСР			:50933	82.246.16.30:52460	3 sec	0 bps	853 B			
	Info	? Unknown	🛕 ТСР			:50933	31.38.111.67:56388	2 sec	0 bps	1.16 KB			
	Info	? Unknown				:49820	84.99.86.26:56795	26 sec	0 bps 🕹	289 B			
	Info	? Unknown	🛕 ТСР	100		:50933	77.147.64.78:55943	1 sec	0 bps —	262 B			
	Info	? Unknown	🛕 ТСР			:50933	77.147.64.78:55944	1 sec	0 bps —	262 B			
	Info	? Unknown	🛕 ТСР			:50933	87.91.126.40:50443	1 sec	0 bps —	390 B			
	Info	? Unknown	🔥 ТСР			:50933	82.245.198.130:56617	1 sec	0 bps	262 B			
	Info	? Unknown	🛕 ТСР			:50933	2.7.143.251:58591	1 sec	0 bps —	134 B			
	Info	2 Unknown				150933	77 147 64 78:56224	4 sec.	0 hns	533 B			



DNS and Infections [1/5]

- The analysis of DNS traffic can be used as a looking glass for spotting infections.
- DGAs (Domain Generation Algorithm) are used i various families of malware to generate rendezvous points for command & control (see previous slide).
- In literature, the first malware using DGAs was Kraken (2008).
- Crypto-locker apps often use DGAs for this purpose.



DNS and Infections [2/5]

- Usually DGAs take as input a seed that is used to generate many pseudo-random domain names.
- The malware keep generating domain names up until there is one registered that is used to connect to the "malware network".
- ntopng can analyse DNS traffic and spot these problems. Note that when we see DNS traffic for DGAs we might have been victim of an attack.



DNS and Infections [3/5]

Examples of DGAs

<IP resolver> <GEO Resolver> <DNS Request>

- a.b.c.d IT Turin afupelalikovacah.com.mydomain.it
- a.b.c.d IT Turin epolowypuvugijys.com.mydomain.it
- a.b.c.d IT Turin uzowawibehezojil.com.mydomain.it
- a.b.c.d IT Turin yfohizihifozoral.com.mydomain.it
- a.b.c.d IT Turin epolowypuvugijys.com.mydomain.it
- a.b.c.d IT Turin uzowawibehezojil.com.mydomain.it
- a.b.c.d IT Turin yfohizihifozoral.com.mydomain.it
- a.b.c.d IT Turin ibpirauljhskybqlfdqnvtpz.ru.mydomain.it
- a.b.c.d IT Turin krmfbypgavgoxklrscbmvolq.ru.mydomain.it
- a.b.c.d IT Turin tkvnjzxlrjnwgeavcnflfsohgkb.ru.mydomain.it
- a.b.c.d IT Turin qusspxmese.mydomain.it
- a.b.c.d IT Turin sxievblqv.mydomain.it
- a.b.c.d IT Turin amsssmy.mydomain.it
- a.b.c.d IT Turin qkbmzxwcshedyprksckrukbnfz.ru.mydomain.it
- a.b.c.d IT Turin riolnodfogydy.mydomain.it
- a.b.c.d IT Turin ufqqzkphnpx.mydomain.it
- a.b.c.d IT Turin oxctpbjzfvf.mydomain.it

def generate_domain(year, month, day):

"""Generates a domain name for the given date.""" domain = ""

for i in range(16):

year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFF0) << 17) month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFF8) day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFE) << 12) domain += chr(((year ^ month ^ day) % 25) + 97)

return domain



DNS and Infections [4/5]

The best approach is start analysing DNS traffic

Active DNS Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info 🗸
Info	DNS 🖒	UDP	:54666	domain	< 1 sec	Cli Server	0 bps —	941 B	xml2.corriereobjects.it ContentServer
Info	DNS 🖒	UDP	:43845	domain	< 1 sec	Clie Server	0 bps —	623 B	xml.corriereobjects.it ContentServer
Info	DNS 🖒	UDP	:53835	domain	< 1 sec	<mark>Cliel</mark> Server	0 bps —	547 B	www.trovoaste.it Generic
Info	DNS 🖒	UDP	:43740	domain	< 1 sec	Clier Server	0 bps —	461 B	www.dday.it FreeTime
Info	DNS 🖒	UDP	:60289	domain	1 sec	Clie Server	0 bps —	563 B	www.corriere.it News
Info	DNS 🖒	UDP	:45126	domain	< 1 sec	Clic Server	0 bps —	716 B	vivimilano.corriere.it News
Info	DNS 🖒	UDP	:48302	domain	< 1 sec	Clier Server	0 bps —	523 B	video.corriere.it News
Info	DNS 🖒	UDP	:39114	domain	< 1 sec	Cliel Server	0 bps —	559 B	vicenza.corriere.it News
Info	DNS 🖒	UDP	:57737	domain	< 1 sec	Cliel Server	0 bps —	555 B	verona.corriere.it News
Info	DNS 🖒	UDP	:57524	domain	< 1 sec	Clie <mark>r Server</mark>	0 bps -	559 B	venezia.corriere.it News

Showing 1 to 10 of 70 rows



Applications T-

Select DNS

10 -

Hosts-



Queries

IP Version





MAC/ARP Monitoring and Scanning [1/2]

- ARP (Address Resolution Protocol) is not used just to bind MAC addresses to IPs, but also for monitoring device presence (e.g. in DHCP networks).
- However it can also be used for scanning networks (e.g. with nmap, fing and other tools).



MAC/ARP Monitoring and Scanning [1/2]

All Layer 2 Devices

ARP Stats

	and the second	and the second second	and a second and the second of		10 - Filte	r MACs- Ma	nufacturer-
Manufacturer	Hosts	ARP Sent♥	ARP Received	Seen Since	Breakdown	Throughput	Traffic
Ubiquiti Networks Inc.	269	38	8	4 min, 32 sec	Sent Ro	9.1 Kbit	4.36 MB
Apple, Inc.	1	10	8	4 min, 32 sec	Se Rovd	8.75 Kbit	4.37 MB
LG ELECTRONICS INC	1	5	2	4 min, 30 sec	Sent P	95.88 bps	14.62 KB
Apple, Inc.	2	5	0	2 min, 16 sec	Sent	361.17 bps	10.22 KB
Apple, Inc.	1	0	0	4 min, 6 sec	Sent	0 bps	2.61 KB
Ubiquiti Networks Inc.	1	0	0	3 min, 30 sec	Sent	0 bps	228 B
n/a	0	0	0	2 min, 24 sec	Sent	0 bps	468 B
Hangzhou Hikvision Digital Technology 20.,Ltd.	1	0	0	4 min, 31 sec	Sent	0 bps	13.6 KB
Ubiquiti Networks Inc.	1	0	0	2 min, 22 sec	Sent	0 bps	1.45 KB
	Manufacturer Ubiquiti Networks Inc. Apple, Inc. LG ELECTRONICS INC Apple, Inc. Apple, Inc. Ubiquiti Networks Inc. n/a Hangzhou Hikvision Digital Technology.co.,Ltd.	ManufacturerHostsUbiquiti Networks Inc.269Apple, Inc.1LG ELECTRONICS INC1Apple, Inc.2Apple, Inc.1Ubiquiti Networks Inc.1n/a0Hangzhou Hikvision Digital Technology .co.,Ltd.1Ubiquiti Networks Inc.1	Manufacturer Hosts ARP Sent ← Ubiquiti Networks Inc. 269 38 Apple, Inc. 1 10 LG ELECTRONICS INC 1 5 Apple, Inc. 2 5 Apple, Inc. 1 0 Ideutiti Networks Inc. 1 0 Namufacture 1 0 Ibiquiti Networks Inc. 1 0 In/a 0 0 Inducture 1 0	Hanufacturer Hosts ARP Sent V ARP Received Lbiquiti Networks Inc. 269 38 8 Apple, Inc. 11 10 8 Apple, Inc. 11 5 2 Apple, Inc. 11 5 2 Apple, Inc. 21 5 0 Apple, Inc. 11 0 0 Ivaliti Networks Inc. 11 0 0	ManufacturerHostsARP Sent VARP ReceivedSeen SinceUbiquiti Networks Inc.2693884 min, 32 secApple, Inc.111084 min, 30 secLG ELECTRONICS INC11524 min, 30 secApple, Inc.2502 secApple, Inc.11004 min, 60 secIbiquiti Networks Inc.11003 secInfactor11003 secInfactor11002 secInfactor11000Infactor11001Infactor11000Infactor11000Infactor11000Infactor11000Infactor11000Infactor11000Infactor11000Infactor110 <t< td=""><td>ManufacturerHostsARP Sent VARP ReceivedSeen SinceBreakdownUbiquiti Networks Inc.2693884 min, 32 secSent RApple, Inc.1110084 min, 32 secSent RLG ELECTRONICS INC11524 min, 30 secSent RApple, Inc.22502 min, 16 secSentApple, Inc.11004 min, 6 secSentApple, Inc.11004 min, 6 secSentApple, Inc.11004 min, 6 secSentManufacturer11004 min, 30 secSentMaple, Inc.11004 min, 30 secSentMaple, Inc.11004 min, 30 secSentMaple, Inc.11003 min, 30 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11001SentMaple, Inc.11004 min, 31 secSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.11</td><td>ManufacturerHostsARP Sent VARP ReceivedSeen SinceBreakdownThroughputUbiquiti Networks Inc.2693884 min, 32 secSent c9.1 KbitApple, Inc.11084 min, 32 secSent c9.5 KbitLG ELECTRONICS INC1524 min, 30 secSent c95.88 bpsApple, Inc.2502 min, 16 secSent c95.81 bpsApple, Inc.1004 min, 6 secSent c95.88 bpsApple, Inc.1003 min, 30 secSent c0 bpsIbiquiti Networks Inc.1003 min, 30 secSent c0 bpsIndacturer1001 min, 4 secSent c0 bpsIndacturer1001 min, 4 secSent c0 bpsIbiquiti Networks Inc.1004 min, 31 secSent c0 bpsIbiquiti Networks Inc.1004 min, 31 secSent c0 bpsIbiquiti Networks Inc.1002 min, 21 secSent c0 bpsIbiquiti Networks Inc.1001 min, 31 secSent c0 bpsIbiquit</td></t<>	ManufacturerHostsARP Sent VARP ReceivedSeen SinceBreakdownUbiquiti Networks Inc.2693884 min, 32 secSent RApple, Inc.1110084 min, 32 secSent RLG ELECTRONICS INC11524 min, 30 secSent RApple, Inc.22502 min, 16 secSentApple, Inc.11004 min, 6 secSentApple, Inc.11004 min, 6 secSentApple, Inc.11004 min, 6 secSentManufacturer11004 min, 30 secSentMaple, Inc.11004 min, 30 secSentMaple, Inc.11004 min, 30 secSentMaple, Inc.11003 min, 30 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11004 min, 31 secSentMaple, Inc.11001SentMaple, Inc.11004 min, 31 secSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.1100SentSentMaple, Inc.11	ManufacturerHostsARP Sent VARP ReceivedSeen SinceBreakdownThroughputUbiquiti Networks Inc.2693884 min, 32 secSent c9.1 KbitApple, Inc.11084 min, 32 secSent c9.5 KbitLG ELECTRONICS INC1524 min, 30 secSent c95.88 bpsApple, Inc.2502 min, 16 secSent c95.81 bpsApple, Inc.1004 min, 6 secSent c95.88 bpsApple, Inc.1003 min, 30 secSent c0 bpsIbiquiti Networks Inc.1003 min, 30 secSent c0 bpsIndacturer1001 min, 4 secSent c0 bpsIndacturer1001 min, 4 secSent c0 bpsIbiquiti Networks Inc.1004 min, 31 secSent c0 bpsIbiquiti Networks Inc.1004 min, 31 secSent c0 bpsIbiquiti Networks Inc.1002 min, 21 secSent c0 bpsIbiquiti Networks Inc.1001 min, 31 secSent c0 bpsIbiquit

Showing 1 to 9 of 9 rows Hosts Monitoring

Mac: 80:2A:A8:8D:69:2C		
MAC Address	80:2A:A8:8D:69:2C (Ubiquiti_8D:69:2) [<u>Show Hosts</u>]	80:2A:A8:8D:69:2C
First / Last Seen	02/04/2017 19:28:54 [4 min, 35 sec ago]	02/04/2017 19:33:26 [3 sec ago]
Sent vs Received Traffic Breakdown	Sent	Rovd
Traffic Sent / Received	5,111 Pkts / 3.71 MB	4,558 Pkts / 666.24 KB
Address Resolution Protocol	ARP Requests	ARP Replies



Detecting TCP Flags-based Attacks [1/2]

- TCP flags distribution can indicate source of problems as in theory you should have a 1:1 ratio for:
 - SYN vs SYN|ACK
 - ICMP ECHO Request vs ECHO Reply
 - ARP Request vs ARP Reply
- TCP FIN vs RST distribution analysis is an interesting parameter for detecting scans.
- ntopng keeps these statistics and it allows alerts to be generated based on these values.



Detecting TCP Flags-based Attacks [2/2]

Interface: eth0	*	Packets	Protocols		<u>_</u> ;;	▲	ľ	Ф	202	SNMP	÷
Ceneral Settings	•	Every Minute	Every	5 Minut	es	Hourl	y	Daily			
Interface Alerts	Interface Alerts Interface eth0										
Rearm minutes		1 The rearm is t	the dead time b	Save etween or	ne alert g	generation	and the	e potential	generat	ion of the ne	xt alert of the same kind.





Detecting Scans

 ntopng has native detection of scans that can be used to detect them regardless of their nature such as SYN scan and Slowloris (low goodput).

General Settings	Every Minu	ite 🌣 Every 5 Minutes 🌣 Hourly 🌣 Daily
Host Alerts		✓ ▲ Trigger alerts for Host ovpn.nic.it
Rearm minutes		1 Image: Save The rearm is the dead time between one alert generation and the potential generation of the next alert of the same kind.
Host Flow Alert Thres	shold	25 Save Max number of new flows/sec over which a host is considered a flooder. Default: 25.
Host SYN Alert Thres	hold	10 Save Max number of sent TCP SYN packets/sec over which a host is considered a flooder. Default: 10.
Host Flows Threshold	ł	32768 Save Max number of flows over which a host is considered a flooder. Default: 32768.



ICMP Traffic Monitoring [1/2]

- ICMP messages are useful for detecting traffic anomalies:
 - ICMP Redirect: MITM, asymmetric path
 - Destination unreachable: network scan?
 - Port unreachable: service scan or a service previously up is now down?
- ntopng is able to monitor ICMP messages and to report issues via alarms it generates on hosts and interfaces.



ICMP Traffic Monitoring [2/2]

ICMP Message	Packets Sent	Last Sent Peer	Packets Received	Last Rcvd Peer	Breakdown	Total
Neighbor Advertisement	4 Pkts	-	0 Pkts		Sent	4 Pkts
Neighbor Solicitation	0 Pkts		4 Pkts	100.00113.1	Rcvd	4 Pkts

ICMP Message	Packets Sent	Last Sent Peer	Packets Received	Last Rcvd Peer	Breakdown	Total
Destination Port Unreachable	103 Pkts	10.00	3 Pkts	-	Sent	106 Pkts
Echo Request	0 Pkts		1 Pkts	10.000	Rcvd	1 Pkts
Echo Reply	1 Pkts	10.111.000.007	0 Pkts		Sent	1 Pkts



Traffic Geolocation [1/2]

- Traffic geolocation is useful for enforcing security rules. Examples:
 - A child iPad is not supposed to access remote countries outside its domain of knowledge
 - A video-surveillance camera can be accessed only by specific ASs/Countries
- ntopng has the ability to geolocate traffic and emit alerts based on continents (i.e. alert if my PC is accessed any Asia or Oceania)



Traffic Geolocation [2/2]

Hosts GeoMap





Monitoring Copyrighted Content [1/4]

University Toolkit

From Wikipedia, the free encyclopedia

University Toolkit is a software package developed by the MPAA for University system administrators to track and log what types of, and how much, traffic goes through their network, and over the internet provided by the University. The toolkit was available for free at www.universitytoolkit.org until a developer for Ubuntu (the operating system which the toolkit is based on) contacted the MPAA and requested that it be taken down,^[1] citing GPL violations, stating that under the GPL, any software must have its source code released under the GPL as well. The MPAA has not released the source code to University Toolkit, despite it being supposedly based entirely on open-source software, specifically snor and ntop.

References [edit]

^ mjg59: Spot the difference
 ^I O

External links [edit]

http://blog.washingtonpost.com/securityfix/2007/11/mpaa_university_toolkit_opens_1.html 2 • •



Monitoring Copyrighted Content [2/4]

 ntopng has the ability to detect L7 protocols by means of nDPI and thus to detect for instance BitTorrent traffic

nt	op			# -	Flows	Hosts - In	terfaces 👻 🚦	¢- ≜-	Q Search Host
Acti	ve Flov	vs							
	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	10 - Applications -
Info	BitTorrent 🖒	TCP	192.168.1.5:49778	ti0042a400-5810.bb.o 🔚 :6858	13 sec	Server	0 bps —	2.88 MB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49783	nlwhalegbit018.xirvi =:51568	12 sec	Server	0 bps —	2.28 MB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49782	80-95-85-191.pool.di =:27961	12 sec	Server	0 bps —	1.91 MB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49796	c-73-8-155-80.hsd1.i 🕮 :6881	9 sec	Server	0 bps —	1003.47 KB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49785	94.196.230.94.threem 📰 :bctp	12 sec	Server	0 bps —	828.33 KB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49787	feralhosting.com 2급 :59905	11 sec	Server	0 bps —	802.31 KB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49792	nqhf166.dediseedbox 🚍 :50726	10 sec	Server	0 bps —	707.02 KB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	TCP	192.168.1.5:49781	balticom-244-108.bal 🚍 :61080	13 sec	Server	0 bps —	517.83 KB	3f19b149f53a50e14fc0b799
Info	BitTorrent 🖒	UDP	192.168.1.5:40959	ryzome.info 🛄 :51413	12 sec	Server	0 bps —	478.25 KB	3f19b149f53a50e14fc0b799
Info	? Unknown	TCP	net031132099127.psko 🖬 :34038	192.168.1.5:40959	11 sec	Client	0 bps —	323.26 KB	

Showing 1 to 10 of 226 rows





Monitoring Copyrighted Content [3/4]

ntop	- Flows	Hosts -	Interfaces -	۰. ي	4 -	Q	Search Host	
Flow: 192.168.1.5:40959 ryzome.info:51413	Overview	÷						

Flow Peers	192.168.1.5:40959 🔁 ryzome.info:51413					
Protocol	UDP / BitTorrent (37)					
First / Last Seen	28/02/2016 09:03:49 [18 min, 26 sec ago] 28/02/2016 09:04:01 [18 min, 14 sec ago]					
Total Traffic	Total: 478.25 KB - Goodput: 456.56 KB (95.5 %) -					
Client vs Server Traffic Breakdown	192 ryzome.info:51413					
Client to Server / Server to Client Traffic	185 Pkts / 12.63 KB -	344 Pkts / 465.62 KB -				
Actual / Peak Throughput	0 bps - / 0 bps					
BitTorrent hash	3f19b149f53a50e14fc0b79926a391896eabab6f					
Dump Flow Traffic						



Monitoring Copyrighted Content [4/4]



89.248.171.130/3f19b149f53a50e14fc0b79926a391896eabab6f -

... face the consequences. You need a client like qBittorrent, Deluge or Transmission to download. info_hash: 3f19b149f53a50e14fc0b79926a391896eabab6f ...

ubuntu-15 10-desktop-amd64 iso apps download - best ... torscan.com/t.php?...3F19B149F53A50E14FC0B79926A391896EABA... -

... copyrighted material isn't. Be careful of what you download or face the consequences. hash: 3F19B149F53A50E14FC0B79926A391896EABAB6F ...

NOTE: This information can be logged onto the database for historical activity tracking.



Unknown vs Unknown

- Unknown traffic does not always mean nDPI needs to be extended to detect a new protocol.
- It can also indicate that there are activities that are worth to be analysed more in detail.

Looking Glass: Unknown Traffic Volume

							ortena*	
IP Address	VLAN	Alerts	Name	Seen Since	Unknown Traffic Volume	Breakdown	Th Upload Vo	lume
••••	0	0	IN RECEIPTION OF COMPANY	1 h, 43 min, 12 sec	342.8 KB	S Rovd	3 Download	Volume
11 ¢	0	0		1 h, 43 min, 12 sec	44.83 KB	<mark>Sen</mark> Rcvd	3 Outgoing I	Flows Count
	0	0	No. 111 No. 1 No. 1 No.	1 h, 42 min, 52 sec	0 B	Sent	5.98 Kbit 🕹	3.56 MB
	0	0	And the second sec	1 h, 42 min, 52 sec	0 B	Sent	0 bps 🕹	1.52 MB
	0	0		1 h, 42 min, 51 sec	0 B	Sent	540.69 bps 🕹	841.73 KB
	0	0	Contraction of the Contraction o	1 h, 42 min, 52 sec	0 B	Sent	0 bps 🕹	721.85 KB
	0	0	TRANSPORT DATABASED IN	1 h, 42 min, 51 sec	0 B	Sent	0 bps 🕹	1.55 MB
	0	0	And the second sec	1 h, 42 min, 52 sec	0 B	Sent	0 bps 🕹	1.54 MB
	0	0	And the second se	1 h, 42 min, 51 sec	0 B	Sent	0 bps 🕹	1.52 MB
	0	0	>]	1 h, 42 min, 51 sec	0 B	Sent	0 bps 🕹	1.52 MB



Critoria ID Varaion

One-way Traffic

- One way traffic can be a good source of information for understanding suspicious activities based on destination and protocol:
 - Multicast traffic can be exploited for disclosing sensitive information (e.g. SSDP, MDNS)
 - TCP traffic is by nature bi-directional, so one-way TCP flow might indicate activities such as probing or service unavailability.
- The flows menu can display one-way flows and spot these situations.



Suspicious Activities Detection

- nDPI can detect over 200 protocols including those that are considered potentially malicious.
- The list includes protocols such as Tor or even long-term acceptable protocols such as SSH or SSL that in certain scenarios can hide something more dangerous such as a VPN.
- Selecting specific protocols (e.g. TOR) in the flow list and sorting them for duration, can enable this analysis.



Characterising Host Risk Factor [1/2]

- Every host can have a security risk associated, depending on the type and nature of traffic it performs.
- nDPI has the ability to cluster layer-7 protocols in families and thus characterise them up.





Characterising Host Risk Factor [2/2]

- However risks are coming not just from traffic that a host makes, but also from ingress traffic.
- As previously said with one-way traffic, this is a good source of understanding the security risk factor a host has associated.



Malware Detection [1/3]

- IDSs have been traditionally used to detect security threats but as traffic is becoming more and more encrypted they are falling short.
- A simple way to effectively monitor malware, is by means of IP blacklists.
- You can configure ntopng to do nightly download of malware hosts and enforce them in ntopng.
- If you use ntopng in monitor mode an alert is reported, in inline-mode instead the communication against such hosts are disabled.



Malware Detection [2/3]

Step I: Enable Malware hosts detection in preferences.

Security Alerts	
Enable Probing Alerts Enable alerts generated when probing attempts are detected.	On Off
Enable Hosts Malware Blacklists Enable alerts generated by traffic sent/received by malware- marked hosts. Overnight new blacklist rules are refreshed.	On Off

https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

• Step 2: See the generated alerts for an overview of malware activities.



Malware Detection [3/3]

Engaged Alerts	Past Alerts	Flow Alerts
Engagoartionto	1 00110110	1101171010

Flow Alerts

				10 - Type- Severity-
Actions	Date/Time	Severity	Alert Type	Description
€ 4 🗎	Thu Feb 16 07:39:38 2017	Error	 Blacklist Host 	blacklisted 71.6.146.185 contacted host [TCP 71.6.146.185:49717 > :902 [proto: 0.0/Unknown][1/1 pkts][60/54 bytes][SYN ACK RST]]
€ A 🗎	Thu Feb 16 08:39:19 2017	Error	 Blacklist Host 	blacklisted 93.174.93.30 contacted host [[TCP 93.174.93.30:29162 > 1 5900 [proto: 0.0/Unknown][1/0 pkts][62/0 bytes][SYN]]
€ A 🗎	Thu Feb 16 09:01:50 2017	Error	Blacklist Host	blacklisted 185.35.62.185 contacted host ri [TCP 185.35.62.185:60205 > :1911 [proto: 0.0/Unknown][1/1 pkts][60/54 bytes][SYN ACK RST]]

Engaged Alerts

Past Alerts Flow Alerts

Past Alerts

10 - Type- Severity-

Actions	Date/Time	Duration	Severity	Alert Type	Description
±	Thu Feb 16 07:39:04 2017	-	Error	Ø Malware Detected	Blacklisted host found 71.6.146.185@0
€ €	Thu Feb 16 08:39:15 2017	-	Error	Ø Malware Detected	Blacklisted host found 93.174.93.30@0
CA B	Thu Feb 16 09:01:48 2017	-	Error	Ø Malware Detected	Blacklisted host found 185.35.62.185@0



Characterising User Traffic [1/5]

- Network administrators should not look at user traffic content as this falls outside of their tasks.
- However detecting (and blocking/shaping/setting a quota) specific protocols not suitable for business usage (e.g. Netflix) can be acceptable.
- Cloud-based services such as Google Drive or DropBox can be prohibited in certain environments so network administrators need a way to know what users are doing (not the data content they are exchanging).



Characterising User Traffic [2/5]

• While nDPI is enough for known what hosts are using what protocols...

All Dropbox Hosts

								10 - Filter Hos	ts- IP Version-
IP Address	Location	Flows	Alerts	Name	Seen Since	ASN	Breakdown	Throughput♥	Traffic
<u>≬</u> ∎∎	Local Host	161	0		2 h, 30 min, 8 sec		S Rcvd	Se Rovd	41.29 Kbit 🕁
	Local Host	2	0	Hore DECREMENTS.	2 h, 30 min, 6 sec		Sent	Sent	0 bps -
	Local Host	4	0		2 h, 29 min, 48 sec		Sent	Sent	0 bps 🕹

 ...inappropriate content (e.g. in schools or public places) cannot be enforced this way as the protocol is generic (e.g. HTTP) but the content is not.



Characterising User Traffic [3/5]

Flash@Start

LA PROTEZIONE INTERNET ITALIANA

- ntopng has been integrated with a content analysis company to complement layer-7 traffic analysis with content enforcement.
- Go to <u>http://flashstart.ntop.org</u> to get your categorisation key.

									10 • Hosts• Appli	cations T - IP vers	on-
	Application	L4 Proto	Client	Server Duration Breakdown Actual Thpt Total		Total Bytes	Info				
Info	HTTP 🖒	TCP	# 1620	www.corriere.it:http	2 min, 23 sec	Clie <mark>t</mark> Server	0 bps -	30.23 KB	/includes2013/SSI/utilit.	News	
Info	HTTP 🖒	TCP	# 11 :41618	www.corriere.it:http	2 min, 21 sec	Client Server	0 bps -	4.13 KB	/includes_methode/cacl	8/ News	
Info	HTTP 🖒	TCP	# 11 :41616	www.corriere.it:http	2 min, 21 sec	Server	0 bps -	33.66 KB	/includes_methode/cacl	8/ News	
Info	HTTP 🖒	TCP	2 :36764	images2.corriereobje	2 min, 17 sec	Client Serve	0 bps -	4.75 KB	/methode_image/placeh	old ContentServer	
Info	HTTP 🖒	🛕 ТСР	60492	static2.vivimilano.c	2 min, 15 sec	Client Serv	0 bps -	2.46 KB	/wp-content/uploads/20	7 News	
Info	HTTP 🖒	🛕 ТСР	60494	static2.vivimilano.c	2 min, 15 sec	Client Serv	0 bps -	2.47 KB	/wp-content/uploads/20	7 News	
Info	HTTP 🖒	🛕 ТСР	11 :36838	images2.corriereobje	2 min, 15 sec	Client Server	0 bps -	1.59 KB	/includes2013/LIBS/css	a ContentServer	
Info	HTTP 🖒	🛕 ТСР	60490	static2.vivimilano.c	2 min, 15 sec	Client Serv	0 bps -	2.46 KB	/wp-content/uploads/20	7 News	
Info	HTTP 🖒	🛕 ТСР	60496	xml2.corriereobjects	2 min, 15 sec	Client Server	0 bps -	1.62 KB	/tools/3a-col-nav/tablet.	ContentServer	
Info	HTTP 🖒	🛕 ТСР	60488	static2.vivimilano.c	2 min, 15 sec	Client Serv	0 bps -	2.44 KB	/wp-content/uploads/20	7 News	



Characterising User Traffic [4/5]

ntop							4	* *	60 -	Flows	Hosts 👻
Interface: bridg	e:en0,en1	*	Packets	Protocols	-	▲		ф	쓭	Traffic Policy	÷
Manage Policies	Bandwid	ith Mana	ager								
Pool Name: Not	Assigned			\$							
Content categories to block :	Adult Ann Association Audio-vide Blog Books Chat Company	1 D	All	one							

Protocol	Traffic to Not Assigned	Traffic fro		
Default	0 (No Limit)	0 (No Limit)		



Characterising User Traffic [5/5]





Alarms On The Go

Internal Log	
Alerts On Syslog Enable alerts logging on system syslog.	On Off
Slack Integration	
Enable Slack Notification Toggle the alert notification via slack.	On Off
Notification Preference Based On Severity Errors (errors only), Errors and Warnings (errors and warnings, no info), All (every kind of alerts will be notified).	Errors and Warnings All
Notification Sender Username Set the username of the sender of slack notifications	ntopng Webhook
Notification Webhook Send your notification to this slack URL	
Nagios Integration	
Send Alerts To Nagios Enable sending ntopng alerts to Nagios NSCA (Nagios Service Check Acceptor).	On Off



Conclusions

- Traffic flow analysis and extraction of metadata information are the cornerstones of network security analysis.
- ntopng is able to provide insights not just for traffic monitoring but also from the security viewpoint.
- The nDPI engine allows traffic to be properly classified and bound to applications.
- Traffic categorization allows traffic patterns to be built not just for tagging traffic but also for malware analysis.

