รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

1 เมษายน – 30 มิถุนายน 2558

1. <u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- ขยายจุดบริการ LAN เพิ่มตามระบบแจ้งซ่อมฯ จำนวน 40 จุด ที่ ห้องประชุม 4 อาคารวิชาการ 1, ห้องประชุมอาคารเครื่องมือ 1, อาคารสุรพัฒน์ 1

1.2 สรุปการดำเนินการบนระบบเครือข่าย ไร้สาย SUT-wifi

- (มิถุนายน 2558) ติดตั้ง AccessPoint เพิ่มที่ชั้น 2-3 อาคารวิชาการ 1 จำนวน 8 เครื่อง
- เปลี่ยน AccessPoint เป็นรุ่นใหม่ที่อาคารเครื่องมือ 5 จำนวน 2 เครื่อง
- ติดตั้ง AccessPoint เพิ่มที่อาคารสุรพัฒน์ 2 จำนวน 2 เครื่อง พร้อมกับเปลี่ยน Switch POE เพื่อรองรับการเพิ่มจำนวน AP. ที่มากขึ้น

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- (เมษายน 2558) วันที่ 11 เมษายน ไฟดับ เครื่อง gen ไม่ทำงาน มีผลให้ harddisk server เสีย 2 ลูก (HP Blade-suthpcc)+HP1Tb (HPDL180-nasnetwork) และ power supply เสีย 1 ตัว ของระบบ suthpcc (compute0-1) ได้ดำเนินการแจ้งเคลมเรียบร้อยแล้ว

1.4 สรุปการดำเนินการบนระบบโทรศัพท์

- เปิดเบอร์ภายในใหม่ 26 เลขหมาย เพื่อรองรับผู้ใช้งานที่เพิ่มมากขึ้น
- จัดซื้อ IP-Phone จำนวน 1 ระบบ ประกอบด้วย software และ หัวเครื่อง IP-Phone จำนวน 22 เครื่อง เพื่อทดลองใช้งานระบบ IP-Phone บนระบบเครือข่าย

1.5การดำเนินการอื่นๆ

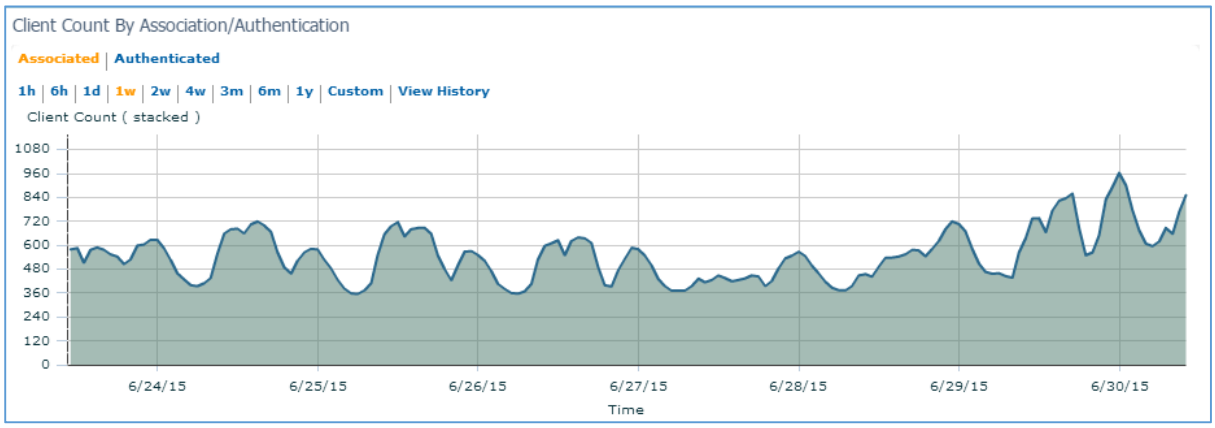
- (เมษายน 2558) จัดทำ Checklist แบบฟอร์มการตรวจสอบระบบเครือข่ายรายวัน
- (เมษายน 2558) จัดทำคู่มือการปฏิบัติงานฝ่ายเครือข่าย
- (เมษายน 2558) จัดสรรพื้นที่เว็บไซต์งานประชุมวิชาการ International and National Conference on Engineering Education http://www.incee13.sut.ac.th/

- (พฤษภาคม 2558) จัดสรรพื้นที่เว็บไซต์สำหรับงานประชุมนานาชาติและการประชุมกรรมการบริหารสมาคม AUAP ได้แก่ www.auap-ishouconbas.sut.ac.th และ www.auap-comu2016.sut.ac.th
- (พฤษภาคม 2558) จัดทำระบบแจ้งเตือนไวรัสและมัลแวร์ http://web.sut.ac.th/ccs/antivirus/

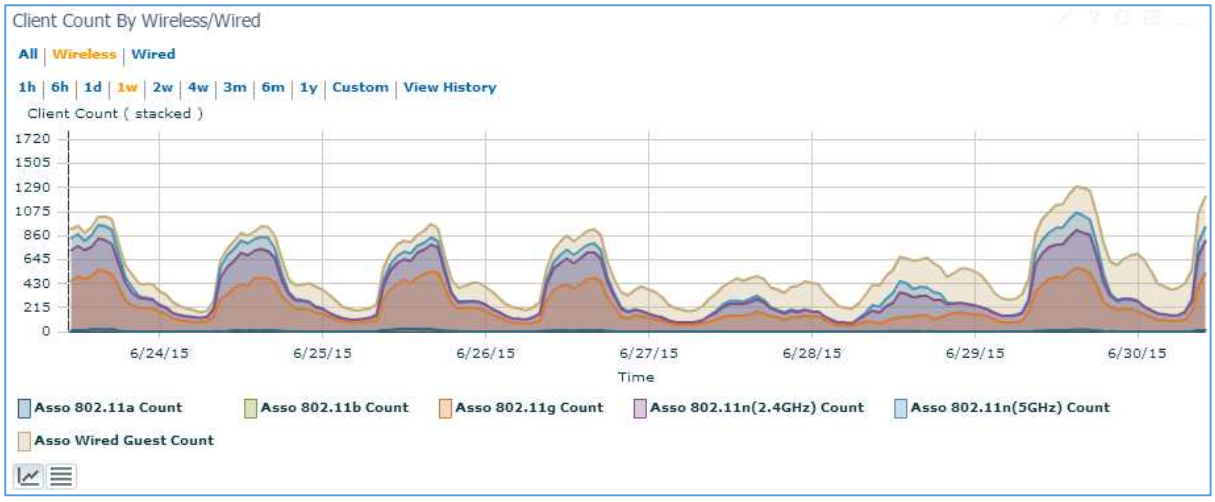
พร้อมทั้งแจ้งเตือนและประชาสัมพันธ์ผู้ใช้งาน และทำการ block เครื่องที่ติดไวรัสและส่ง packet ก่อกวนระบบเครือข่าย

- (มิถุนายน 2558) เพิ่ม VPN Account สำหรับสถาบันวิจัยแสงซินโครตรอน 7 account ทำให้มีผู้ใช้งาน SUTVPN จากสถาบันวิจัยแสงซินโครตรอน จำนวน 98 account
- (มิถุนายน 2558) จัดสรร internet account จำนวน 400 account สำหรับงานประชุมวิชาการ WUTC และ SEATUC
- (มิถุนายน 2558) จัดสรรพื้นที่เว็บไซต์ สำหรับสำนักวิชาทันตแพทยศาสตร์ http://dent.sut.ac.th
- (มิถุนายน 2558) เปิดตัวบริการ SUT-WEBEx https://sut.webex.com ซึ่งเป็นระบบ Web Conference ใช้งานผ่าน web browser หรือใช้งานผ่าน application Cisco WebEx Social ได้ทั้ง iphone ipad และ Android โดยมหาวิทยาลัยสามารถประยุกตใช้งานในการประชุมทางไกล หรือการเรียนการสอนผ่านอินเตอรเน็ต เป็นการสื่อสารแบบ real-time ที่รองรับไดทั้งภาพวีดีโอ เสียง รวมไปถึงการแลกเปลี่ยนขอมูล การทำ presentation และยังสามารถทำงานร่วมกับ applications อื่นๆอีกมากมาย

2.รายงานการใช้งาน ระบบเครือข่ายไร้สาย (SUT-wifi)



รูปภาพแสดงการใช้งาน WIFI ในโซนหอพักนักศึกษา ตัวอย่างข้อมูลตั้งแต่วันที่ 24-30 มิถุนายน 2558 (ที่มา : Cisco Prime : 203.158.4.209)



รูปภาพแสดงการใช้งาน WIFI ในโซนอาคารเรียน-สำนักงานและกลุ่มอาคารเครื่องมือ ตัวอย่างข้อมูลตั้งแต่วันที่ 24-30 มิถุนายน 2558 (ที่มา : Cisco Prime : 203.158.4.208)

3.รายงานสรุปสถานการณ์ของ traffic internet

มหาวิทยาลัยมีช่องทางออกอินเตอร์เน็ตปัจจุบันดังนี้

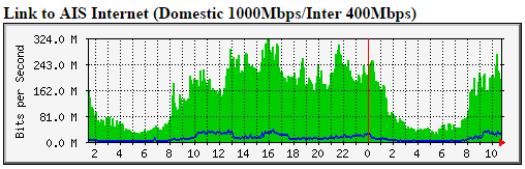
ช่องทางที่ 1 ผ่านเครือข่าย UNINET ที่ความเร็ว 2 Gigabit (ความเร็ว Domestic และ Inter กำหนดโดย UNINET)

ช่องทางที่ 2 ผ่าน Internet Provider บริษัท AIS TRUE Corp. ที่ความเร็ว 1 Gbps/400 Mbps (international/Domestic)

3.1กราฟแสดงปริมาณการใช้งานเครือข่ายอินเทอร์เน็ต (Internet Traffic)

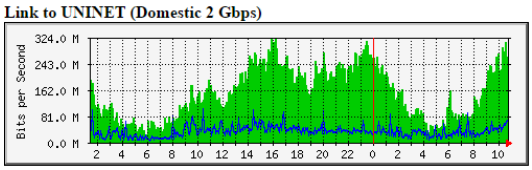
ตัวอย่างข้อมูล ณ วันที่ 30 มิถุนายน 2558

- การแสดงผลรายวัน (ผ่านช่องทางทาง AIS)



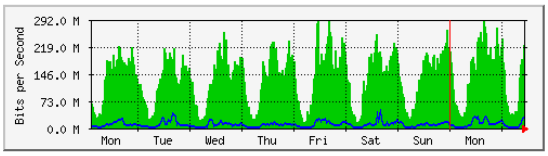
	Max	Average	Current
In	321.8 Mb/s (3.2%)	140.5 Mb/s (1.4%)	222.0 Mb/s (2.2%)
Out	35.8 Mb/s (0.4%)	11.0 Mb/s (0.1%)	26.0 Mb/s (0.3%)

- การแสดงผลรายวัน (ผ่านช่องทางทาง Uninet)



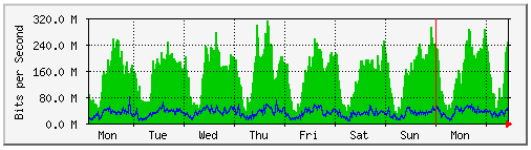
	Max	Average	Current
In	323.6 Mb/s (16.2%)	150.4 Mb/s (7.5%)	226.4 Mb/s (11.3%)
Out	100.8 Mb/s (5.0%)	33.1 Mb/s (1.7%)	55.8 Mb/s (2.8%)

- แสดงผลแบบรายสัปดาห์ (ผ่านช่องทาง AIS)



	Max	Average	Current
In	290.8 Mb/s (2.9%)	136.3 Mb/s (1.4%)	223.7 Mb/s (2.2%)
Out	48.0 Mb/s (0.5%)	9578.7 kb/s (0.1%)	24.2 Mb/s (0.2%)

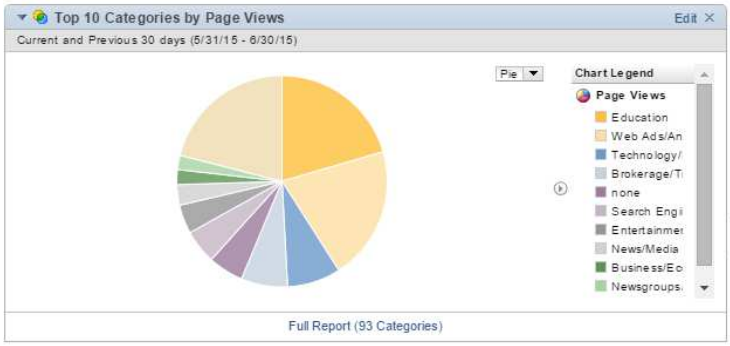
- แสดงผลแบบรายสัปดาห์ (ผ่านช่องทาง Uninet)



	Max	Average	Current
In	312.7 Mb/s (15.6%)	152.9 Mb/s (7.6%)	249.0 Mb/s (12.5%)
Out	77.8 Mb/s (3.9%)	31.0 Mb/s (1.6%)	48.0 Mb/s (2.4%)

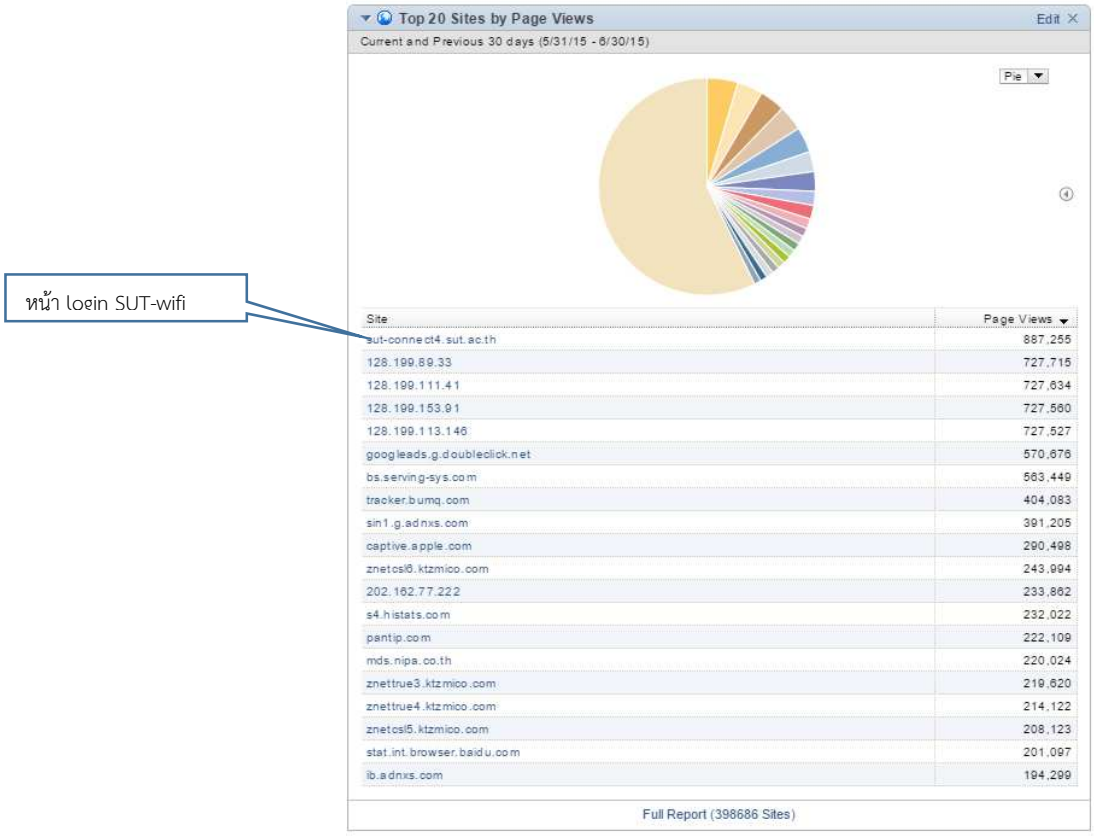
3.2 สรุปตามลักษณะการใช้งาน

- แยกตาม Categories สูงสุด 10 อันดับ



รูปภาพแสดงการใช้งาน internet แยกตาม Categories ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 31 พฤษภาคม 2558- 30 มิถุนายน 2558 (ที่มา : Bluecoat Reporter : 203.158.4.203)

- แยกตามเว็บไซต์ที่มีการใช้งานสูงสุด 20 อันดับ



Site	Page Views
sut-connect4.sut.ac.th	887,255
128.199.89.33	727,715
128.199.111.41	727,634
128.199.153.91	727,560
128.199.113.146	727,527
googleads.g.doubleclick.net	570,676
bs.serving-sys.com	563,449
tracker.bumq.com	404,083
sin1.g.adnxs.com	391,205
captive.apple.com	290,498
znetcsl8.ktzmico.com	243,994
202.162.77.222	233,862
s4.histats.com	232,022
pantip.com	222,109
mds.nipa.co.th	220,024
znettrue3.ktzmico.com	219,620
znettrue4.ktzmico.com	214,122
znetcsl5.ktzmico.com	208,123
stat.int.browser.baidu.com	201,097
ib.adnxs.com	194,299

รูปภาพแสดงการใช้งาน internet แยกตามเว็บไซต์ที่มีการใช้งานสูงสุด20อันดับ ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 31 พฤษภาคม 2558- 30 มิถุนายน 2558 (ที่มา : Bluecoat Reporter : 203.158.4.203)

- แยกตาม Application สูงสุด 25 อันดับ

Application — Applications

	Risk	Application Name	Sessions	Bytes	Threats
1	4	dns	409.4 M	87.8 G	0
2	4	web-browsing	206.3 M	22030.7 G	457.5 K
3	4	ssl	198.5 M	155711.5 G	7
4	4	facebook-base	131.2 M	12347.3 G	0
5	2	ping	14.3 M	1.6 G	0
6	2	instagram-base	9.6 M	837.7 G	0
7	2	twitter-base	7.5 M	536.0 G	0
8	1	naver-line	7.2 M	838.0 G	0
9	5	bittorrent	4.6 M	19.5 G	0
10	4	web-crawler	4.6 M	671.4 G	14
11	2	google-analytics	4.1 M	39.1 G	403
12	4	youtube-base	3.8 M	3994.1 G	6
13	1	apple-maps	3.6 M	238.5 G	0
14	2	kerberos	3.3 M	7.3 G	0
15	5	http-video	3.3 M	13878.6 G	0
16	5	skype	2.8 M	179.5 G	0
17	1	insufficient-data	2.3 M	1.5 G	0
18	3	facebook-chat	2.3 M	595.8 G	0
19	2	ntp	2.2 M	445.1 M	0
20	0	instagram	2.2 M	208.3 G	0
21	2	icloud-base	2.1 M	26.8 G	0
22	3	ms-sms	1.8 M	23.8 G	0
23	3	itunes-base	1.8 M	120.7 G	1
24	1	apple-push-notifications	1.8 M	18.5 G	0
25	4	dailymotion	1.7 M	2523.4 G	0

รูปภาพแสดงการใช้งาน internet แยกตาม Application ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 31 พฤษภาคม 2558- 30 มิถุนายน 2558 (ที่มา : Paloato : 203.158.4.110)

3.3 สรุปสถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย

Malware Intrusions

	Message	Count
	APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com	134
	APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn (1:28069)	16
	MALWARE-CNC Win.Dropper.Ch variant outbound connection (1:32670)	15
-1	MALWARE-CNC Win.Trojan.Adload.dyhq variant outbound connection (1:29828)	11
	MALWARE-CNC Win.Trojan.Ramnit variant outbound detected (1:33600)	10
-2	BLACKLIST DNS request for known malware domain megabrowse.biz -	8
-2	BLACKLIST DNS request for known malware domain qualitink.net - Win.Trojan.Mudrop	5
-2	BLACKLIST User-Agent known malicious user agent BOT/0.1 (1:21925)	5
	MALWARE-CNC Win.Trojan.Sality variant outbound connection (1:19964)	5
	BLACKLIST DNS request for known malware domain outobox.net - Win.Trojan.Mudrop	3
-3	BLACKLIST User-Agent known malicious user agent - Post (1:24111)	2
	MALWARE-CNC Win.Trojan.Badur variant outbound connection (1:31683)	2
	MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:25050)	1
	MALWARE-OTHER self-signed SSL certificate with default Internet Widgits Pty Ltd	1

Last updated 24 minutes ago

รูปภาพแสดงชนิดมัลแวร์ที่ระบาดภายในเครือข่ายมหาวิทยาลัย ข้อมูล ณ วันที่ 30 มิถุนายน 2558 (ที่มา : 203.158.4.43)

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	CRITICAL	Suspicious.Gen Command And Control Traffic	13591	spyware	893
2	CRITICAL	Suspicious.Gen Command And Control Traffic	13990	spyware	429
3	MEDIUM	SCAN: Host Sweep	8002	scan	12
4	CRITICAL	UDP Flood	8502	flood	3
5	MEDIUM	Vmprotect User-Agent Traffic	10064	spyware	3
6	MEDIUM	Virus/Win32.WGeneric.evozj	238...	virus	2
7	MEDIUM	Virus/Android.WGeneric.flkpk	102...	virus	2
8	MEDIUM	Suspicious DNS Query (conficker:wdbpfyzuh.org)	406...	spyware	1
9	MEDIUM	Suspicious DNS Query (conficker:zjjfjcunit.ws)	406...	spyware	1
10	MEDIUM	Suspicious DNS Query (conficker:gmlsrbr.cc)	406...	spyware	1
11	MEDIUM	Suspicious DNS Query (conficker:rmeaqq.net)	406...	spyware	1
12	MEDIUM	Suspicious DNS Query (conficker:vgjiuluyd.biz)	406...	spyware	1
13	MEDIUM	Suspicious DNS Query (conficker:qnpxuhgk.ws)	406...	spyware	1
14	MEDIUM	Suspicious DNS Query (conficker:wjlaa.info)	406...	spyware	1
15	MEDIUM	Suspicious DNS Query (conficker:skokerksp.org)	406...	spyware	1
16	MEDIUM	Suspicious DNS Query (conficker:elrauojvcdk.net)	406...	spyware	1
17	MEDIUM	Suspicious DNS Query (conficker:renulaahjvv.com)	406...	spyware	1
18	MEDIUM	Suspicious DNS Query (conficker:hdgmudc.net)	406...	spyware	1
19	MEDIUM	Suspicious DNS Query (conficker:vdeaxzdemh.cc)	406...	spyware	1
20	MEDIUM	Suspicious DNS Query (conficker:dujzzs.cn)	406...	spyware	1
21	MEDIUM	Suspicious DNS Query (conficker:tyztqeo.info)	406...	spyware	1
22	MEDIUM	Suspicious DNS Query (conficker:eokrug.ws)	406...	spyware	1
23	MEDIUM	Suspicious DNS Query (conficker:vznfibdfynf.com)	406...	spyware	1
24	MEDIUM	Suspicious DNS Query (conficker:zfdrpsv.cc)	406...	spyware	1
25	MEDIUM	Suspicious DNS Query (conficker:lbbscvgggj.info)	406...	spyware	1

ภาพแสดงภัยคุกคามจากไวรัสและspy ware ซึ่งถูก Drop ได้จาก firewall ข้อมูล ณ วันที่ 30 มิถุนายน 2558 (ที่มา : Firewall : 203.158.4.110)

Top Attackers (High Impact Events)

	Source IP	Count
	203.158.4.228	130
	192.168.130.25	89
	203.158.4.225	64
	203.158.4.230	51
	192.168.144.31	39
	203.158.4.231	26
	172.31.4.250	19
	172.32.68.3	15
	172.31.12.192	14
	172.32.160.177	12
-1	172.32.165.36	11
-1	172.32.168.217	9
-1	203.158.4.226	8
+1	203.158.4.46	7
	172.32.77.19	6
-1	192.168.29.3	6
-1	192.168.116.109	6
	203.158.4.45	6
	172.31.146.80	4
	172.32.68.168	4

Last updated 10 minutes ago

รูปภาพแสดง หมายเลข ip ผู้ติดไวรัส และส่ง packet ก่อกวนระบบเครือข่าย ข้อมูล ณ วันที่ 30 มิถุนายน 2558 (ที่มา : 203.158.4.43)