รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

1 กรกฎาคม – 30 กันยายน 2558

1. <u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>

1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- (กรกฎาคม 2558) ตรวจพบปัญหา response time จากการ ping ใช้เวลามากเกินไป เกิดจาก switch 3com ที่ฟาร์มมหาวิทยาลัย ส่ง error packet ออกมาจำนวนมาก แก้ไขโดยเปลี่ยน switch ตัวใหม่เป็น cisco เรียบร้อยแล้ว
- (กรกฎาคม 2558) upgrade firmware switch POE รุ่น SG300 เป็น versionใหม่ เพื่อให้ support voice QOS
- (กรกฎาคม 2558) ไฟดับ 15 นาที ส่งผลให้ทราบว่า ups อาคาร c1 ชั้น 2 ตู้หลัก, อาคาร a ชั้น2 ตู้หลัก แบตเสื่อมสภาพไม่สามารถจ่ายกระแสไปหล่อเลี้ยงอุปกรณ์ได้
- (กรกฎาคม 2558) มีการติดตั้งอุปกรณ์ source fire เป็นอุปกรณ์ประเภท IPS เพื่อตรวจสอบ packet ในระบบ Network และยับยั้งการโจมตีระบบเครือข่ายในรูปแบบต่างๆ เช่น DDOs-attack virus trojan เป็นต้น
- (สิงหาคม 2558) มีการจัดทำแผน MA อุปกรณ์ระบบเครือข่าย (กันยายน -ตุลาคม 2558) เพื่อตรวจเชคและบำรุงรักษาอุปกรณ์เครือข่าย ตามสถานที่ต่าง ๆ
- (กันยายน 2558) ปรับเปลี่ยนความเร็วช่องสัญญาณ internet โดยจะมีการเพิ่มช่องสัญญาณ internet (Domestic/International) จากเดิม 1 Gbps/400 Mbps เป็น 2 Gbps/1 Gbps) ซึ่งจะสามารถรองรับผู้ใช้บริการได้มากขึ้น

1.2 สรุปการดำเนินการบนระบบเครือข่าย ไร้สาย SUT-wifi

- ติดตั้ง access point เพิ่มเติม ที่
  อาคารบริหาร จำนวน 1 เครื่อง,
  อาคารวิชาการ 1 จำนวน 4 เครื่อง,
  อาคารบรรณสาร จำนวน 3 เครื่อง,
  อาคารเครื่องมือ 1-6 จำนวน 4 เครื่อง
  ศูนย์นวัตกรรม จำนวน 2 เครื่อง
- เปลี่ยน access point เป็นรุ่นใหม่แทนรุ่น AIR-AP1231G-E-K9
  อาคารบริหาร จำนวน 3 เครื่อง,

อาคารบรรณสาร1-2 จำนวน3 เครื่อง,
ฟาร์ม มทส จำนวน 4 เครื่อง,
หอพักนักศึกษา 1-12 จำนวน 36 เครื่อง,
หอพักนักศึกษา 14B จำนวน 3 เครื่อง,
อาคารสุรพัฒน์ 1 จำนวน 5 เครื่อง,
อาคารเครื่องมือ 1-6 จำนวน 16 เครื่อง,
ศูนย์นวัตกรรม จำนวน 6 เครื่อง,
อาคารกิจกรรมนักศึกษา จำนวน 4 เครื่อง,
สนามแบดมินตัน สนามบาสเก็ตบอล สนามฟุตบอล และสำนักงานเก่าสถานกีฬา จำนวน 5 เครื่อง,
สำนักงาน รปภ.(ประตู 1) จำนวน 1 เครื่อง,
อาคารกาญจนาภิเษก จำนวน 1 เครื่อง

1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- (กรกฎาคม 2558) Harddisk Bluecoat (203.158.4.226) ซึ่งทำหน้าที่เป็น proxy server เสีย 1 ลูก ได้ดำเนินการแจ้งเคลมเรียบร้อยแล้ว
- (กรกฎาคม 2558) แอร์ Denko เสีย มีอาการมอเตอร์เสีย ประสานงานกับส่วนอาคาร ได้เข้ามาทำการแก้ไขเรียบร้อยแล้ว
- (กรกฎาคม 2558) บริษัท SBN แจ้งดำเนินการปรับปรุงแนวสาย Fiber Optic ตอนนอกใหม่ เพื่อเพิ่มประสิทธิภาพมากยิ่งขึ้น
- (กันยายน 2558) Harddisk Bluecoat (203.158.4.227) เสีย1ลูก ได้ดำเนินการแจ้งเคลมเปลี่ยนลูกใหม่เรียบร้อยแล้ว

1.4 สรุปการดำเนินการบนระบบโทรศัพท์

- (กรกฎาคม 2558) ทดสอบใช้งาน IP-Phone , Jabber Application
- (กรกฎาคม 2558) ตั้งค่าการเชื่อมต่ออุปกรณ์โทรศัพท์ ระหว่าง PABX Acatel กับ ตู้สาขาของ cisco เพื่อทดลองการใช้งานระบบ ip phone ช่วงแรกยังพบปัญหาลูกค้าโทรมา ไม่ได้ยินเสียเจ้าหน้าที่ปลายทาง และมีอาการหลุดบ่อยครั้ง ซึ่งได้รับการแก้ไขแล้ว
- (กรกฎาคม 2558) ทดสอบใช้งาน IP-Phone , Jabber Application เมื่อทำการ call ผ่าน Jabber พบ Iphone ยังพบปัญหาลูกค้าโทรมา ไม่ได้ยินเสียเจ้าหน้าที่ปลายทาง
- (กันยายน 2558) เปลี่ยนผู้ให้บริการเหมาโทรศัพท์ตัด 8 จาก TOT เป็น AIS โดยจะมีการเชื่อมต่อ link E-1 ของ AIS กับตู้ PABX Acatel เพื่อให้สามารถโทรเข้า-ออกภายนอกมหาวิทยาลัยได้ด้วยการตัด 8 (ทดแทน link TOT)

1.5การดำเนินการอื่นๆ

- (กรกฎาคม 2558) เพิ่ม internet account นักศึกษา-บัณฑิตศึกษา รหัส 58 จำนวน 4,337 account
- (กรกฎาคม 2558) เพิ่ม internet account สำหรับโครงการห้องเรียนวิทยาศาสตร์ 60 account
- (กรกฎาคม 2558) disable internet account นักศึกษาที่มีสถานะ สำเร็จการศึกษา -พ้นสภาพ
- (กรกฎาคม 2558) แจ้งเตือน website pemc.sut.ac.th ถูก hack sql injection
- (กรกฎาคม 2558) sutmail ไม่สามารถรับส่งเมลล์ได้ตามปกติ เมลล์ค้างอยู่ที่ mailgate way ไม่สามารถส่งถึง sutmail ได้ โดยค้างอยู่สูงสุด 7000 กว่าฉบับ ตรวจสอบไม่พบความผิดของอุปกรณ์ mailgateway และ กลุ่ม server sutmail แต่เมื่อ2-3วันก่อนมีการทดสอบ อุปกรณ์ IPS ตัวใหม่ (Sourcefire) คาดว่าน่าจะมีส่วนทำให้เมลล์ไม่สามารถส่งถึงกันได้ เจ้าหน้าที่จึงทดลองปิด firewall ตัวใหม่ เมลล์จึงสามารถทยอยส่งถึง inbox ผู้ใช้ได้ตามปรกติ
- (กรกฎาคม 2558) ทดสอบเปิดการทำงาน IPS ตัวใหม่ อีกครั้ง พบว่ามี effect กับ mail gateway และระบบเมลล์จริง แม้จะอยู่ใน mode monitoring เฉยๆ โดยมีเมลล์คิวที่ค้างอยู่ ไม่สามารถรับส่งได้เพิ่มขึ้นจำนวนมากแก้ไขโดยเปลี่ยน ip ของ mailgateway เพื่อหลีกเลี่ยง traffic mail ผ่านอุปกรณ์ Sourcefire
- (กรกฎาคม 2558) ประชาสัมพันธ์ แจ้งสถานะการณ์แพร่ระบาดของไวรัสและมัลแวร์ของมหาวิทยาลัยที่โจมตีระบบเครือข่าย และ block เครื่องที่ติดไวรัส-มัลแวร์ โดยเครื่องที่ติดไวรัสจะส่ง packet ก่อกวนระบบเครือข่ายและโจมตีเครื่อง server
- (สิงหาคม 2558) จัดสรร internat account จำนวน 60 account สำหรับกิจกรรม AFM-II
- (สิงหาคม 2558) จัดสรร internat account จำนวน 15 account สำหรับคณะกรรมการประเมินคุณภาพการศึกษาภายใน
- (สิงหาคม 2558) สร้างเว็บไซต์ its.sut.ac.th เพื่อเป็นเว็บไซต์ฝ่ายเครือข่าย ศูนย์คอมพิวเตอร์
- (สิงหาคม 2558) เผยแพร่ข้อมูลเกี่ยวกับ พรบ. ตัวใหม่ คือ พรบ.ลิขสิทธิ์ 2558 บนเว็บไซต์ its.sut.ac.th
- (กันยายน 2558) จัดสรร internet account จำนวน 500 account ในงานมหกรรมนวัตกรรมไทย สำหรับใช้งานวันที่ 22-27 กันยายน 2558

- (กันยายน 2558) แจ้งเตือนผู้ใช้งานระบบ email ให้พึงระวังการคลิ้ก link ใดๆ ตลอดจนการเปิดไฟล์แนบจดหมายจากคนที่ไม่รู้จัก /รวมถึง link ในเว็บไซต์ต่างๆ ที่ไม่น่าเชื่อถือ ซึ่งเป็นภัยคุกคามประเภทใหม่ มีชื่อว่า Ransomware หรือ software เรียกค่าไถ่
- (กันยายน 2558) แก้ไข เว็บ biomass ถูก hack และมีการนำไฟล์ phishing เข้ามาวางบนเว็บไซต์ เพื่อเอาข้อมูลบัตรเครดิตลูกค้า -จึงทำการแก้ไข permission ใหม่ และแจ้งเตือน webmasterให้เฝ้าระวัง
- (กันยายน 2558) เครื่องแม่ข่าย student.sut.ac.th ถูกฝังสคริปยิงเมลล์ ทำให้พื้นที่เต็มไม่สามารถใช้บริการได้ แก้ไขโดยตรวจสอบ และเอาสคริปที่ยิงออกจาก web hosting และ clear mail queue ทั้งหมด
- (กันยายน 2558) จัดสรรพื้นที่เว็บไซต์ สำหรับงาน 20 ปีไอที ของสาขาวิชาเทคโนโลยีสารสนเทศ (soctech.sut.ac.th/it/20IT)

2.รายงานการใช้งาน ระบบเครือข่ายไร้สาย (SUT-wifi)

ตารางแสดงจำนวนผู้ใช้งานระบบ sut-wifi ทั้งหมด ตัวอย่างข้อมูล 4 สัปดาห์ย้อนหลัง (เมื่อวันที่ 8 สิงหาคม – 27 กันยายน 2558)

time	Authen from 203.158.4.209	Authen from 203.158.4.210	Total per day
08/31/2015 ;11:59:59	2298	2961	5259
09/01/2015 ;11:59:59	2353	2776	5129
09/02/2015 ;11:59:59	2516	2560	5076
09/03/2015 ;11:59:59	2297	2775	5072
09/04/2015 ;11:59:59	1957	2722	4679
09/05/2015 ;11:59:59	1367	2012	3379
09/06/2015 ;11:59:59	1837	2538	4375
09/07/2015 ;11:59:59	2699	2762	5461
09/08/2015 ;11:59:59	2956	2798	5754
09/09/2015 ;11:59:59	2811	2677	5488
09/10/2015 ;11:59:59	2697	2730	5427
09/11/2015 ;11:59:59	2367	2749	5166
09/12/2015 ;11:59:59	1457	2268	3725
09/13/2015 ;11:59:59	1890	2628	4518
09/14/2015 ;11:59:59	2853	2759	5612
09/15/2015 ;11:59:59	2667	2848	5515
09/16/2015 ;11:59:59	2687	2902	5589
09/17/2015 ;11:59:59	2723	2884	5607
09/18/2015 ;11:59:59	2337	2186	4523
09/19/2015 ;11:59:59	1543	2241	3784
09/20/2015 ;11:59:59	1939	2252	4191

09/21/2015 ;11:59:59	2658	2887	5515
09/22/2015 ;11:59:59	2715	2895	5610
09/23/2015 ;11:59:59	2503	2817	5320
09/24/2015 ;11:59:59	2766	2792	5558
09/25/2015 ;11:59:59	2170	2759	4929
09/26/2015 ;11:59:59	1779	2143	3922
09/27/2015 ;11:59:59	1837	2717	4554

(ที่มา : cisco prime 203.158.4.209-210)

สรุป จำนวนผู้ใช้งานเฉลี่ยต่อวัน 4954 คน ต่อวัน

จำนวนผู้ใช้งานสูงสุด 5754 คน ต่อวัน

จำนวนผู้ใช้งานต่ำสุด 3725 คน ต่อวัน

3.รายงานสรุปสถานการณ์ของ traffic internet

มหาวิทยาลัยมีช่องทางออกอินเตอร์เน็ตปัจจุบันดังนี้

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

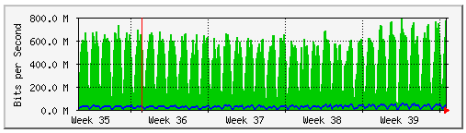
ช่องทางที่ 2 ผ่าน Internet Provider บริษัท AIS TRUE Corp. ที่ความเร็ว 2 Gbps/1 Gbps (international/Domestic) (*ปรับเปลี่ยนความเร็วช่องสัญญาณ internet เมื่อวันที่ 29 กันยายน 2558 จากเดิม1 Gbps/400 Mbps เป็น 2 Gbps/1 Gbps)

3.1กราฟแสดงปริมาณการใช้งานเครือข่ายอินเทอร์เน็ต (Internet Traffic)

ตัวอย่างข้อมูล ย้อนหลัง 1 เดือน (วันที่27 สิงหาคม- 28 กันยายน 2558) ที่มา : mrtg.sut.ac.th

- **การแสดงผลรายเดือน (ผ่านช่องทางทาง AIS)**

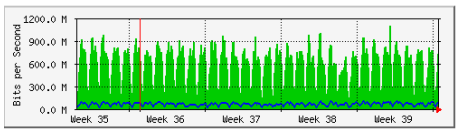
`Monthly' Graph (2 Hour Average)



	Max	Average	Current
In	797.2 Mb/s (8.0%)	444.3 Mb/s (4.4%)	773.7 Mb/s (7.7%)
Out	51.3 Mb/s (0.5%)	23.7 Mb/s (0.2%)	42.9 Mb/s (0.4%)

- **การแสดงผลรายเดือน (ผ่านช่องทางทาง Uninet)**

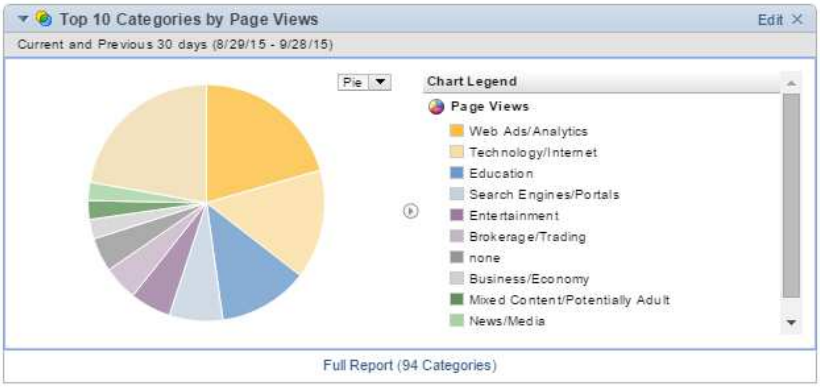
`Monthly' Graph (2 Hour Average)



	Max	Average	Current
In	1094.8 Mb/s (54.7%)	579.9 Mb/s (29.0%)	721.4 Mb/s (36.1%)
Out	103.0 Mb/s (5.1%)	59.2 Mb/s (3.0%)	71.4 Mb/s (3.6%)

3.2 สรุปตามลักษณะการใช้งาน ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 29 สิงหาคม 2558- 28 กันยายน 2558 (ที่มา : Bluecoat Reporter : 203.158.4.200)

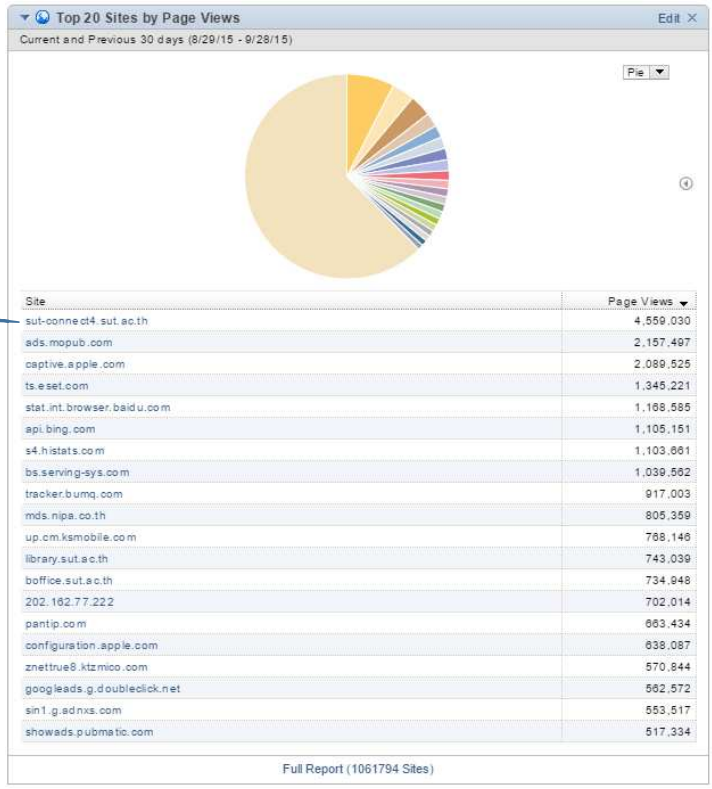
- แยกตาม Categories สูงสุด 10 อันดับ



รูปภาพแสดงการใช้งาน internet แยกตาม Categories

- แยกตามเว็บไซต์ที่มีการใช้งานสูงสุด 20 อันดับ

หน้า login SUT-wifi



Site	Page Views
sut-connect4.sut.ac.th	4,559,030
ads.mopub.com	2,157,497
captive.apple.com	2,089,525
ts.eset.com	1,345,221
stat.int.browser.baidu.com	1,168,585
api.bing.com	1,105,151
s4.histats.com	1,103,661
bs.serving-sys.com	1,039,562
tracker.bumq.com	917,003
mds.nipa.co.th	805,359
up.cm.ksmobile.com	768,146
library.sut.ac.th	743,039
boffice.sut.ac.th	734,948
202.162.77.222	702,014
pantip.com	663,434
configuration.apple.com	638,087
znettrue8.ktzmico.com	570,844
googleads.g.doubleclick.net	562,572
sin1.g.adnxs.com	553,517
showads.pubmatic.com	517,334

รูปภาพแสดงการใช้งาน internet แยกตามเว็บไซต์ที่มีการใช้งานสูงสุด 20 อันดับ

- **แยกตาม Application สูงสุด 25 อันดับ** ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 29 สิงหาคม 2558- 28 กันยายน 2558

Application — Applications

	Risk	Application Name	Sessions	Bytes	Threats
1	4	dns	501.7 M	111.9 G	0
2	4	ssl	289.9 M	193400.1 G	8
3	4	facebook-base	251.4 M	28707.0 G	0
4	4	web-browsing	243.6 M	23605.6 G	893.1 K
5	2	instagram-base	18.3 M	1603.4 G	0
6	2	ping	14.4 M	2.0 G	0
7	1	naver-line	11.7 M	1185.4 G	0
8	2	twitter-base	10.3 M	919.3 G	0
9	1	insufficient-data	7.7 M	6.1 G	0
10	5	bittorrent	7.6 M	3.0 G	0
11	4	web-crawler	6.6 M	731.8 G	113
12	2	google-analytics	5.6 M	43.6 G	285
13	1	apple-maps	5.5 M	130.9 G	0
14	4	ms-update	4.4 M	1063.1 G	0
15	5	google-docs-base	4.1 M	16697.9 G	0
16	3	itunes-base	4.0 M	629.8 G	0
17	2	icloud-base	4.0 M	80.0 G	0
18	5	http-video	3.9 M	20777.6 G	0
19	4	facebook-video	3.8 M	7181.0 G	0
20	4	youtube-base	3.8 M	4923.6 G	2
21	2	kerberos	3.4 M	7.4 G	0
22	2	ntp	3.3 M	829.3 M	0
23	1	apple-push-notifications	3.1 M	34.2 G	0
24	3	facebook-chat	3.0 M	1054.4 G	0
25	4	ssh	2.7 M	388.4 G	0

รูปภาพแสดงการใช้งาน internet แยกตาม Application (ที่มา : Paloato : 203.158.4.110)

4. สรุปภัยคุกคามระบบเครือข่าย ข้อมูลเก็บรวบรวมตั้งแต่วันที่ 29 สิงหาคม 2558- 28 กันยายน 2558 (ที่มา Sourcefire : 203.158.4.43)

4.1สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย

Malware Intrusions

Message	Count
APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com	75,531
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030)	32,719
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549)	28,933
APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn (1:28069)	25,237
MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023)	15,494
MALWARE-CNC Win.Trojan.Necurs variant outbound detection (1:31299)	11,950
MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746)	10,479
MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496)	10,458
MALWARE-CNC Win.Trojan.Kazy outbound connection (1:35462)	6,224
BLACKLIST User-Agent known malicious user agent - Post (1:24111)	4,895
BLACKLIST User-Agent known malicious user agent - OSSProxy (1:5760)	4,059
BLACKLIST DNS request for known malware domain erwbtkidthetcwerc.com (1:28058)	2,964
BLACKLIST DNS request for known malware domain rterybrstutnrsbberve.com (1:28059)	2,957
MALWARE-BACKDOOR Win.Trojan.GGDoor.22 variant outbound connection (1:19747)	2,779
BLACKLIST DNS request for known malware domain rybwtbeitwjeitv.com (1:28060)	2,566
MALWARE-CNC Win.Trojan.Sality variant outbound connection (1:19964)	2,264
MALWARE-CNC Win.Backdoor.Iniduoh variant outbound connection (1:28817)	2,029
BLACKLIST DNS request for known malware domain restless.su - Gamarue Trojan	2,015
MALWARE-CNC Win.Rootkit.Necurs outbound connection (1:31070)	1,764
BLACKLIST User-Agent known malicious user-agent string update - Win.Trojan.Waski	1,220

Last updated 8 minutes ago

รูปภาพแสดง มัลแวร์บนระบบเครือข่ายภายในมหาวิทยาลัย

4.2 **เครื่องที่ส่ง packet โจมตีระบบเครือข่ายสูงสุด**

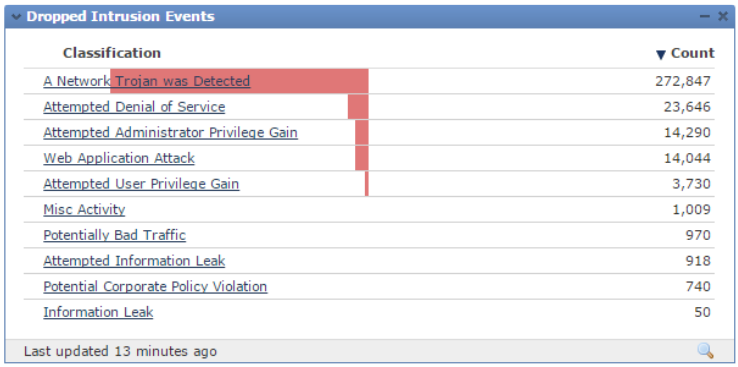
Top Attackers (High Impact Events)

Source IP	Count
203.158.4.225	37,976
203.158.4.229	35,204
203.158.4.230	31,991
2001:3c8:c301:200::230	16,036
203.158.4.231	8,439
172.32.191.205	4,595
203.158.4.226	2,977
203.158.4.45	2,854
172.31.30.218	2,822
192.168.124.14	2,716
203.158.4.228	2,451
172.32.175.60	2,061
203.158.4.46	1,948
203.158.4.227	1,846
172.32.189.190	1,400
172.32.107.187	1,323
172.32.163.209	1,256
172.31.30.209	1,237
172.32.28.52	1,125
172.32.170.65	1,091

Last updated 6 minutes ago

รูปภาพแสดง หมายเลข ip ผู้ติดไวรัส และส่ง packet ก่อกวนระบบ

4.3. การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS (Sourcefire: 203.158.4.43)



Dropped Intrusion Events

Classification	Count
A Network Trojan was Detected	272,847
Attempted Denial of Service	23,646
Attempted Administrator Privilege Gain	14,290
Web Application Attack	14,044
Attempted User Privilege Gain	3,730
Misc Activity	1,009
Potentially Bad Traffic	970
Attempted Information Leak	918
Potential Corporate Policy Violation	740
Information Leak	50

Last updated 13 minutes ago

รูปภาพแสดงการยับยั้งการโจมตีระบบเครือข่าย โดยอุปกรณ์ Source fire

4.4 **การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Firewall** (Paloato.158.4.110)

Threat Prevention — Threats

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	CRITICAL	Suspicious.Gen Command And Control Traffic	13591	spyware	734.0 K
2	MEDIUM	SCAN: Host Sweep	8002	scan	213.7 K
3	CRITICAL	Suspicious.Gen Command And Control Traffic	13990	spyware	74.0 K
4	CRITICAL	Suspicious.Gen Command And Control Traffic	13585	spyware	19.2 K
5	MEDIUM	Backdoor.Win32.GGDoor.22	12581	spyware	18.7 K
6	CRITICAL	Suspicious.Gen Command And Control Traffic	14155	spyware	8.7 K
7	MEDIUM	Virus/Win32.WGeneric.esfkq	280...	virus	7.6 K
8	MEDIUM	SCAN: TCP Port Scan	8001	scan	5.9 K
9	MEDIUM	Virus/Win32.WGeneric.ffgbs	286...	virus	5.0 K
10	MEDIUM	Suspicious user-agent strings	10004	spyware	4.2 K
11	MEDIUM	Vmprotect User-Agent Traffic	10064	spyware	3.8 K
12	CRITICAL	UDP Flood	8502	flood	2.4 K
13	CRITICAL	Suspicious.Gen Command And Control Traffic	14542	spyware	1.3 K
14	CRITICAL	WGeneric.Gen Command And Control Traffic	14535	spyware	1.2 K
15	MEDIUM	Nsanti User-Agent Traffic	10028	spyware	1.1 K
16	MEDIUM	Virus/Win32.WGeneric.fjivl	223...	virus	860
17	MEDIUM	HackTool/Win32.keygen.aul	202...	virus	660
18	CRITICAL	WGeneric.Gen Command And Control Traffic	14712	spyware	626
19	CRITICAL	Suspicious.Gen Command And Control Traffic	13716	spyware	553
20	MEDIUM	Virus/Win32.sality.czefx	225...	virus	492
21	MEDIUM	Virus/Win32.WGeneric.gapkp	220...	virus	481
22	MEDIUM	Suspicious DNS Query (generic:coooau.com)	402...	spyware	440
23	MEDIUM	kovter.Gen Command And Control Traffic	14733	spyware	405
24	CRITICAL	Suspicious.Gen Command And Control Traffic	13717	spyware	390
25	MEDIUM	Suspicious DNS Query (generic:tfoddnzuinck.info)	400...	spyware	334

รูปภาพแสดงการยับยั้งการโจมตีระบบเครือข่าย โดยอุปกรณ์ Firewall (Paloato.158.4.110)