# รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

## 1 พฤษภาคม – 31 พฤษภาคม 2560

1. **<u>รายงานการดำเนินงานของฝ่ายเครือข่าย</u>**

### 1.1 สรุปการดำเนินการบนระบบเครือข่าย SUTnet

- ปรับปรุงระบบเครือข่าย LAN และ Wifi ส่วนประสานงานมทส-กทม. โดยใช้งาน internet ผ่านระบบผ่านช่องทาง Uninet ยกเลิกการใช้งาน internet ผ่าน ADSL ทำให้มีความเร็วสูงขึ้น ระบบมีความเสถียรมากขึ้น
- Fiber optic บริเวณอาคารสุรสัมนาคาร 2 ถูกตัดขาด เนื่องจากมีการลอกท่อร่องระบายน้ำ แล้วมีการตัดท่อร้อยสาย fiber optic ที่อยู่ในร่องระบายน้ำออก โดยช่างสุรสัมนาคารอ้างว่าขวางทางน้ำ เรื่องอยู่ในระหว่างการหาแนวทางแก้ไขปัญหา -ประเมินราคาซ่อม
- นำอุปกรณ์ switch cisco รุ่น WS-C2960X-24TS-LL ติดตั้งหน่วยประสานงานมทส-กทม. 1ตัว
- นำอุปกรณ์ switch cisco ติดตั้ง ณ ห้องสัมมนา 3 อาคารเรียนรวม 1 จำนวน 1ตัว

### 1.2 สรุปการดำเนินการบนระบบเครือข่ายไร้สาย SUT-wifi

- อาคารเรียนรวม 1 มี access point รุ่น AIR-AP1832I-S-K9 เสีย 1 ตัว นำอุปกรณ์ใหม่ติดทดแทน และส่งอุปกรณ์เก่าเคลมบริษัทเรียบร้อยแล้ว

### 1.3 สรุปการดำเนินการบนระบบ Internet Data Center

- แก้ไขปัญหาระบบจัดเก็บข้อมูลชนิด VSAN โดยระบบ VSAN2 มี warning เกี่ยวกับมีปัญหา COMPONENT METADATA HEALTH – LOCATING PROBLEMATIC DISK ของ vmserver0 แก้ไขโดยสั่ง full migrate vmserver0 และทำการลบ disk group ของ vmsareve0 ออก แล้วแบ่ง diskgroup ใหม่ ทำให้สามารถใช้งานได้ตามปกติ
- แก้ไขปัญหา vmserver31 ขึ้นไอคอนไฟกระพริบสีแดง ตรวจสอบไม่พบความผิดปรกติ แก้ไขโดย shutdown virtual machine ภายใต้ vmserver31 (ประกอบด้วย bmx2.sut.ac.th, cas2.sut.ac.th) จากนั้น shutdown server31 แล้วถอดปลั๊กเพื่อตัดไปหล่อเลี้ยง จากนั้นเสียบปลั๊กและstart vmserver31 ใหม่
- เครื่อง vmserver5 มีปัญหา boot ไม่ขึ้น แก้ไขโดย reinstall ESXi ใหม่ (แบบ upgrade) และตั้งค่า bios boot order ใหม่

- Patch windows server ให้เป็นปัจจุบัน เพื่อป้องกันมัลแวร์ Wonnacry ประกอบด้วย active directory profiler1-4 และ space, DNS server, DHCH server, Mail server 6 ตัว, web server 2 ตัว ทั้งนี้ได้ประชาสัมพันธ์ให้ผู้ดูแล server ของหน่วยงานภายใน update patch เรียบร้อยแล้ว
- จัดสรร virtual server ให้หอสมุดเบญญาลัย ระบบปฏิบัติการ windows server : windows 2012 R2 standard (64 bit), processor : 4 Vcpu, ram 8 Gb, พื้นที่จัดเก็บข้อมูล C: 100 Gb / D : 2 Tb

**1.4 สรุปการดำเนินการบนระบบโทรศัพท์**

- โทรศัพท์ของ TOT ขัดข้องโดยตรวจสอบพบสาย fiber optic ขาด ทำให้ภายนอกไม่สามารถโทรเข้าเบอร์ภายในมหาวิทยาลัยได้ แต่การโทรออกยังสามารถใช้งานได้ตามปกติ ทั้งนี้งานเครือข่ายฯ ได้ประสานงานบริษัท TOT เพื่อดำเนินการแก้ไขปัญหาดังกล่าวเรียบร้อยแล้ว
- ปรับปรุงระบบโทรศัพท์ส่วนหน้า**ให้รองรับระบบ** IP-Phone ซึ่งสามารถทำ Feature ต่างๆ ในการใช้บริการโทรศัพท์ หรือ ประชุม VDO Call ได้ ทำให้มหาวิทยาลัย**ประหยัดค่าใช้จ่ายโทรศัพท์**ในการติดต่อประสานงานระหว่างหน่วยงานภายในมหาวิทยาลัยฯ กับสำนักงานส่วนหน้า

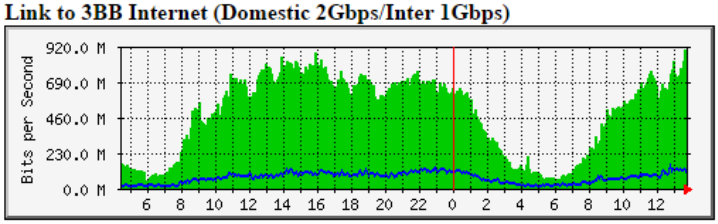
**1.5การดำเนินการอื่นๆ**

- สร้างระบบ infographics เพื่อรวบรวม infographics ของฝ่าย ที่ http://its.sut.ac.th/infograph
- จัดสรร internet account สำหรับเจ้าหน้าที่สตง. 10 account
- จัดสรร internet account โครงการพัฒนาสื่อการเรียนรู้เพื่อพัฒนาคุณภาพการศึกษาด้านวิทยาศาสตร์ 22 account
- จัดสรร internet account สำหรับกิจกรรมโครงการแข่งขันออกแบบและสร้างหุ่นยนต์แห่งประเทศไทย 71 account
- จัดสรร internet account สำหรับนักเรียน โรงเรียนสุรวิวัฒน์ ม.1 และ ม.4 จำนวน 86 account
- จัดสรร internet account สำหรับอาจารย์พิเศษ โรงเรียนสุรวิวัฒน์ 5account
- ตรวจสอบการ hack เว็บไซต์ส่วนพัสดุ พร้อมวิธีแก้ไข-แนวทางป้องกัน
- ประกาศแจ้งเตือนมัลแวร์ Wana Decrypt0r 2.0 พร้อมวิธีการป้องกัน

## 2.รายงานการใช้งานระบบเครือข่าย

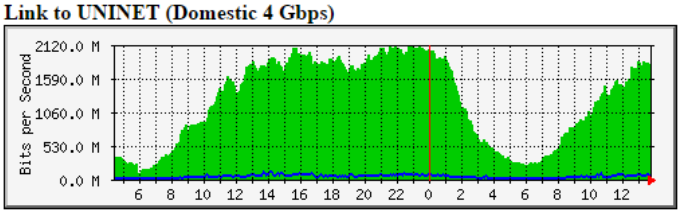
### Internet Gateway Traffic

**Link to 3BB Internet (Domestic 2Gbps/Inter 1Gbps)**



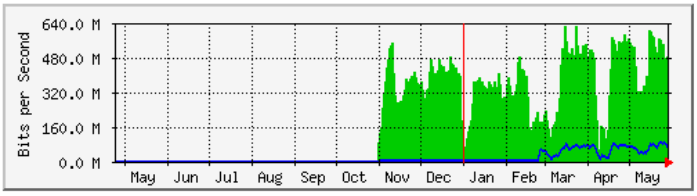

| | Max | Average | Current |
|---|---|---|---|
| In | 893.0 Mb/s (8.9%) | 483.8 Mb/s (4.8%) | 825.7 Mb/s (8.3%) |
| Out | 156.2 Mb/s (1.6%) | 67.9 Mb/s (0.7%) | 117.3 Mb/s (1.2%) |

**Link to UNINET (Domestic 4 Gbps)**



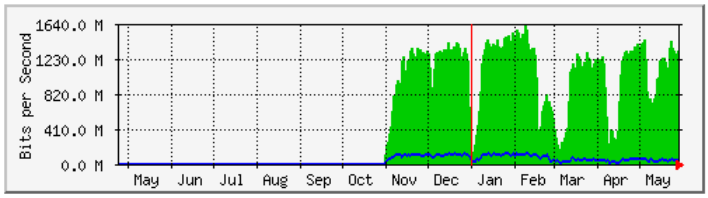

| | Max | Average | Current |
|---|---|---|---|
| In | 2116.8 Mb/s (21.2%) | 1230.9 Mb/s (12.3%) | 1709.5 Mb/s (17.1%) |
| Out | 122.7 Mb/s (1.2%) | 39.9 Mb/s (0.4%) | 51.7 Mb/s (0.5%) |

**`Yearly' Graph (1 Day Average)**




| | Max | Average | Current |
|---|---|---|---|
| In | 623.9 Mb/s (6.2%) | 365.4 Mb/s (3.7%) | 481.0 Mb/s (4.8%) |
| Out | 86.0 Mb/s (0.9%) | 24.8 Mb/s (0.2%) | 68.6 Mb/s (0.7%) |

**`Yearly' Graph (1 Day Average)**




| | Max | Average | Current |
|---|---|---|---|
| In | 1609.6 Mb/s (16.1%) | 1054.7 Mb/s (10.5%) | 1326.1 Mb/s (13.3%) |
| Out | 126.6 Mb/s (1.3%) | 70.1 Mb/s (0.7%) | 43.2 Mb/s (0.4%) |

*ทางออก Uninet 4Gbps / 3BB Domestic 2 Gbps,Inter 1 Gbps) / ข้อมูล ณ วันที่ 30 พ.ค. 60

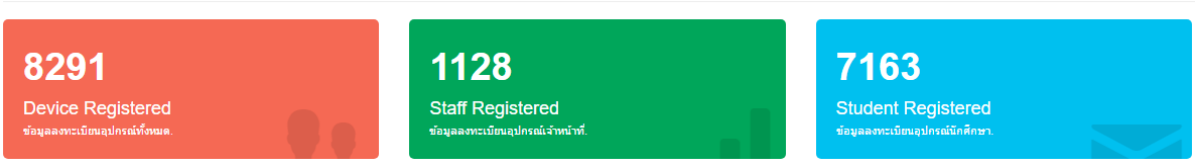
### 2.1 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมฯ)

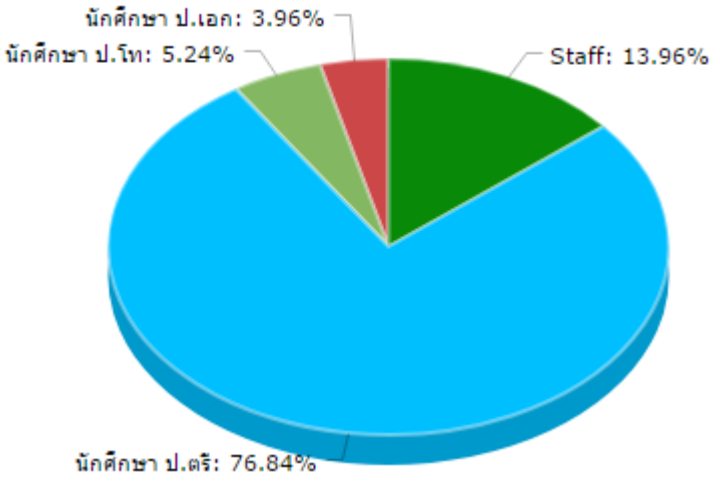
(ข้อมูล ณ วันที่ 30 พ.ค. 60)

| วิธีการ | จำนวน |
|---|---|
| วิธีการแบบ NAC In-Band | 280 คน |
| วิธีการแบบ ISE | 1458 คน |
| **รวมทั้งหมด** | **1,733 คน** |

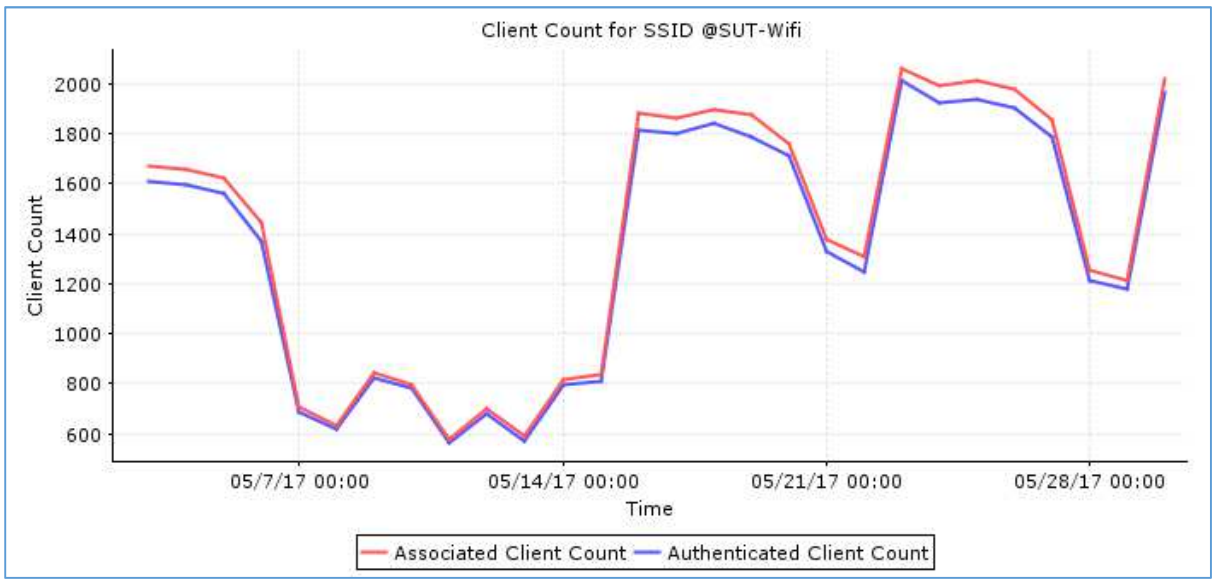
## 2.2 รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

### 2.2.1 จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi (ข้อมูล ณ วันที่ 30 พ.ค. 60)

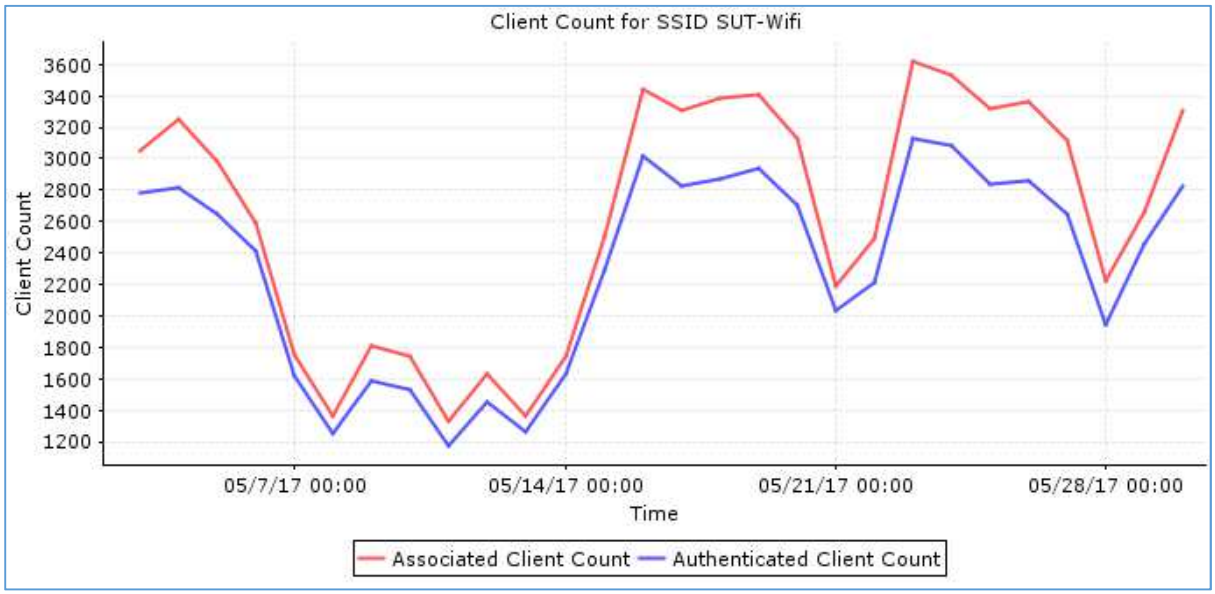


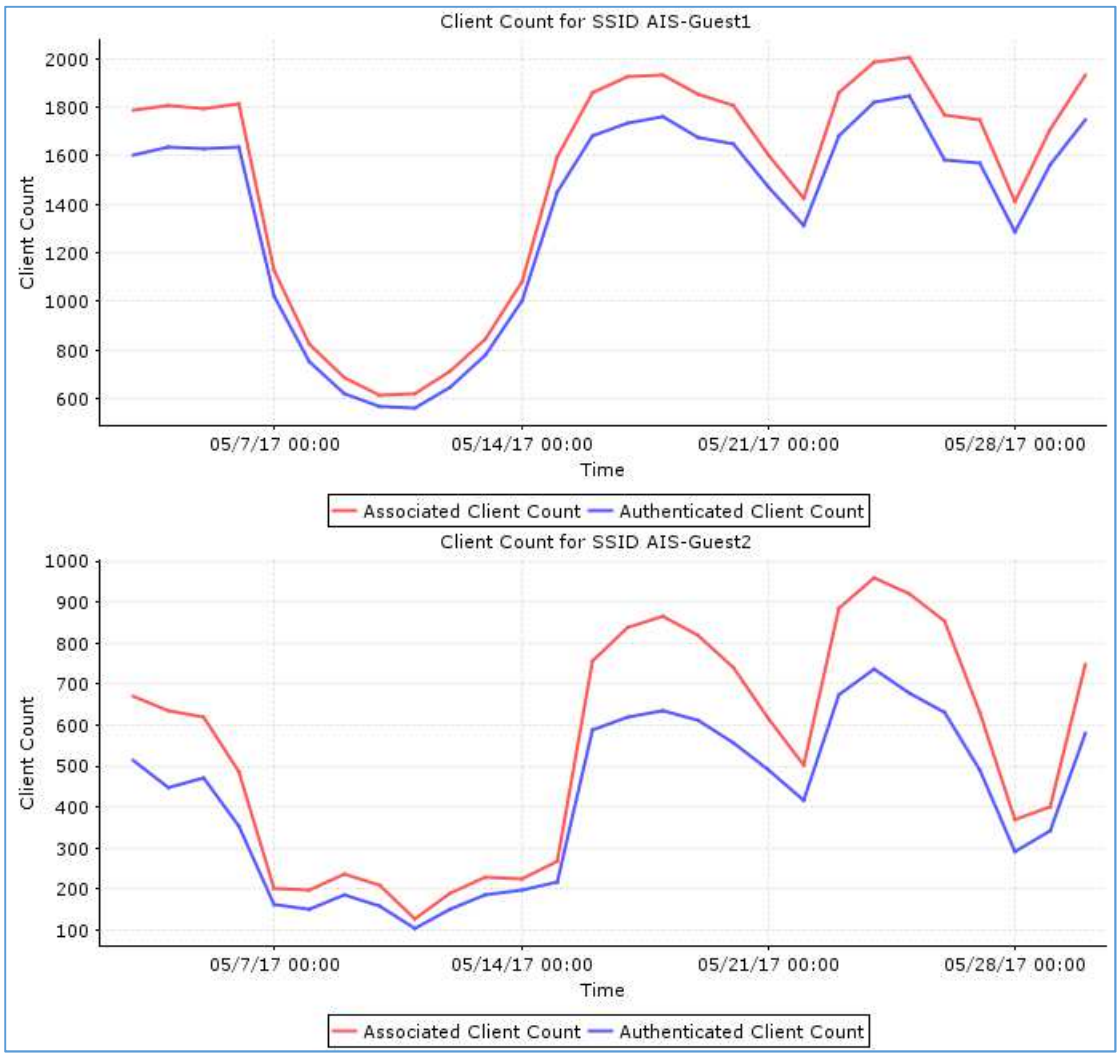

จำนวนผู้ใช้งานเครือข่ายไร้สาย @SUT-Wifi (ที่มา https://203.158.4.211) (ข้อมูล 1 เดือนย้อนหลัง)



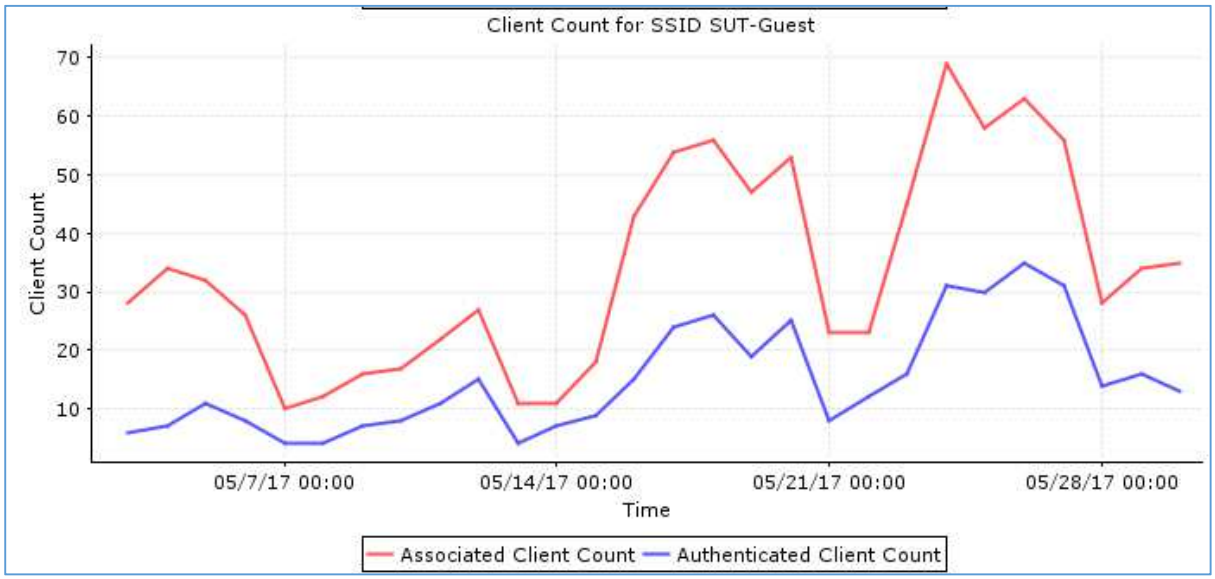
### 2.2.2 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Wifi



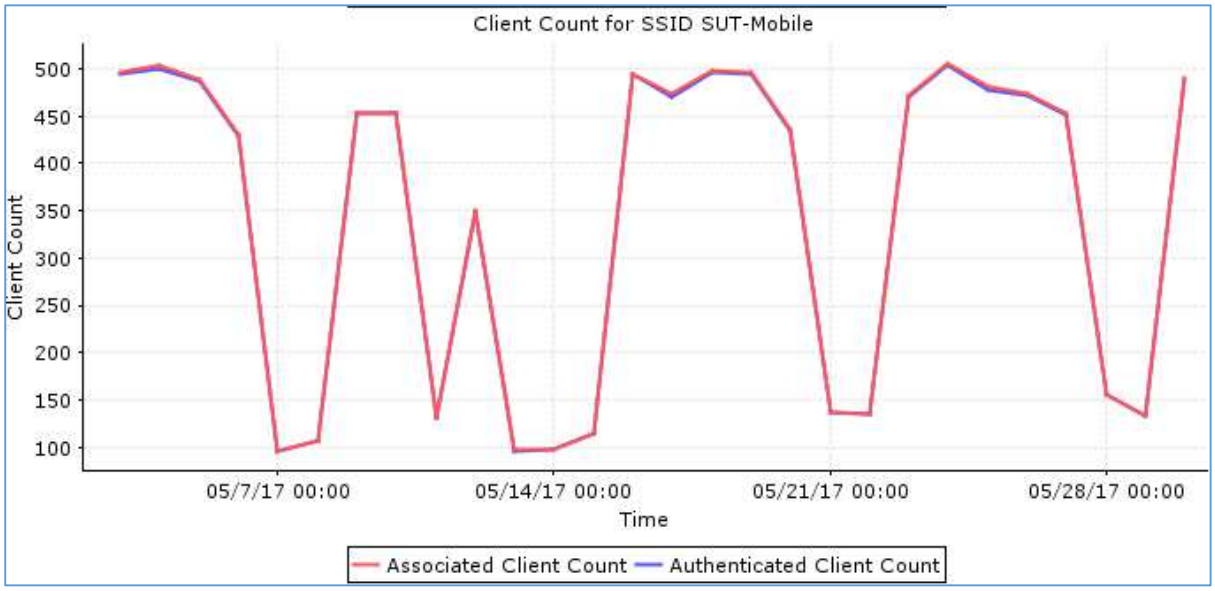

### 2.2.3 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-AIS



### 2.2.4 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Guest




### 2.2.5 จำนวนผู้ใช้งานเครือข่ายไร้สาย SUT-Mobile




ที่มา https://203.158.4.211 (ข้อมูล 1 เดือนย้อนหลัง)

### 2.2.6 สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

- ผู้ใช้งานผ่านระบบ wireless สูงสุด 8,101 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless ต่ำสุด 2,532 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 5,810.79 คน/วัน

## 3. ภัยคุกคามระบบเครือข่าย

- **สถานะการณ์ไวรัสและมัลแวร์ที่แพร่ระบาดในมหาวิทยาลัย** (ข้อมูล 1 เดือนย้อนหลัง)

  **(ที่มา : Sourcefire 203.158.4.43)**

**Malware Intrusions**

| Message | Count |
|---|---|
| +1 MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35030:1) | 158,757 |
| +1 MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35549:1) | 74,082 |
| BLACKLIST suspicious .bit dns query (1:41083:1) | 61,057 |
| +1 MALWARE-CNC Win.Trojan.Njrat variant outbound connection (1:25100:5) | 51,078 |
| -1 MALWARE-CNC Win.Trojan.Andromeda variant outbound connection (1:33496:1) | 28,310 |
| +18 MALWARE-CNC Win.Trojan.Pmabot outbound connection (1:37213:3) | 26,982 |
| BLACKLIST DNS request for known malware domain ltc.give-me-coins.com (1:31660:1) | 24,457 |
| -2 MALWARE-CNC Win.Trojan.Zeus variant outbound connection (1:35746:1) | 23,778 |
| BLACKLIST suspicious .bit tcp dns query (1:42841:1) | 14,375 |
| +2 BLACKLIST DNS request for known malware domain rybwtbeitwieitv.com (1:28060:1) | 13,919 |
| MALWARE-CNC Torpig bot sinkhole server DNS lookup (1:16693:5) | 13,808 |
| +2 BLACKLIST DNS request for known malware domain rterybrstutnrsbberve.com | 13,309 |
| +2 MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection (1:26023:3) | 11,986 |
| -4 BLACKLIST DNS request for known malware domain erwbtkidthetcwerc.com | 11,574 |
| +2 MALWARE-CNC Win.Trojan.Jaktinier outbound connection (1:31459:3) | 11,381 |
| BLACKLIST suspicious .bit tcp dns query (1:42841:3) | 11,248 |
| -6 BLACKLIST DNS request for known malware domain xa.yessearches.com - | 10,434 |
| MALWARE-CNC Win.Trojan.Jenxcus outbound connection attempt with unique User- | 9,984 |
| +3 MALWARE-CNC Win.Trojan.Glupteba.M initial outbound connection (1:30288:2) | 5,025 |
| +1 MALWARE-CNC Win.Trojan.Nvbpass variant outbound connection (1:19864:5) | 4,996 |

Last updated less than a minute ago

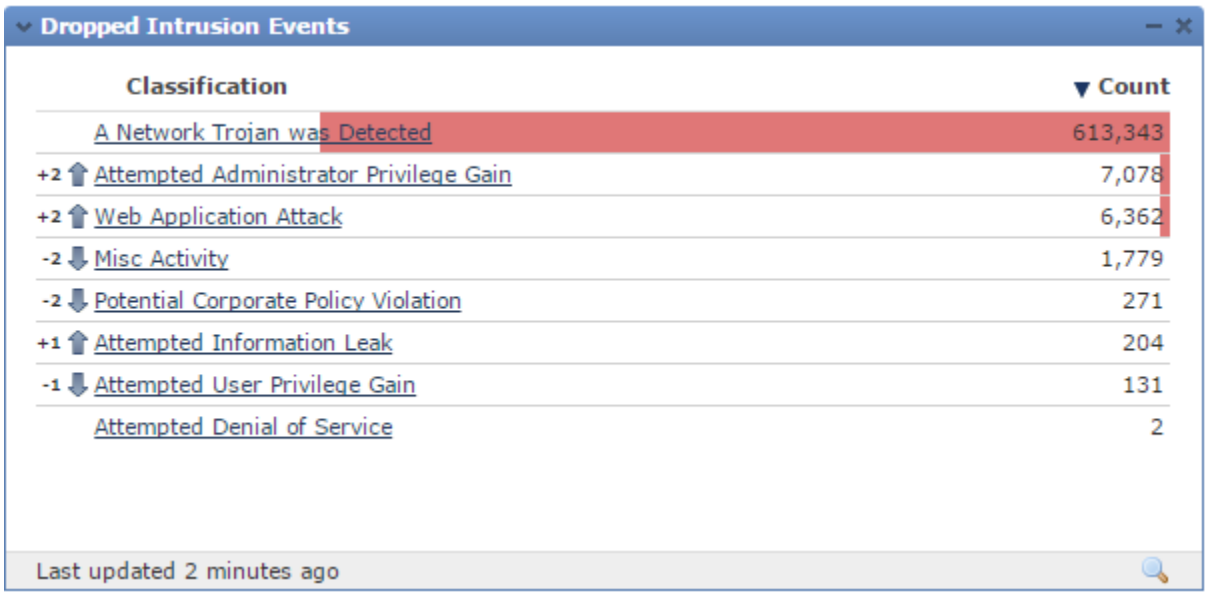
**Top Attackers (High Impact Events)**

| Source IP | Count |
|---|---|
| 203.158.4.46 | 52,100 |
| 203.158.4.230 | 25,874 |
| 203.158.4.45 | 22,369 |
| 203.158.4.225 | 21,679 |
| 172.32.163.230 | 16,148 |
| 192.168.29.10 | 15,532 |
| 172.31.12.246 | 14,117 |
| 172.106.11.10 | 13,353 |
| 172.31.0.45 | 13,264 |
| 2001:3c8:c301:6:250:56ff:febc:341d | 12,689 |
| 203.158.4.229 | 11,821 |
| 172.32.168.222 | 10,946 |
| 10.0.0.88 | 10,310 |
| 192.168.29.5 | 8,924 |
| 192.168.29.4 | 7,492 |
| 172.31.8.228 | 7,168 |
| 172.31.22.182 | 6,974 |
| 172.32.68.197 | 6,801 |
| 172.32.0.113 | 6,187 |
| 192.168.116.49 | 6,117 |

Last updated 1 minute ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ IPS** (ข้อมูล 1 เดือนย้อนหลัง)

  **(ที่มา : Sourcefire 203.158.4.43)**



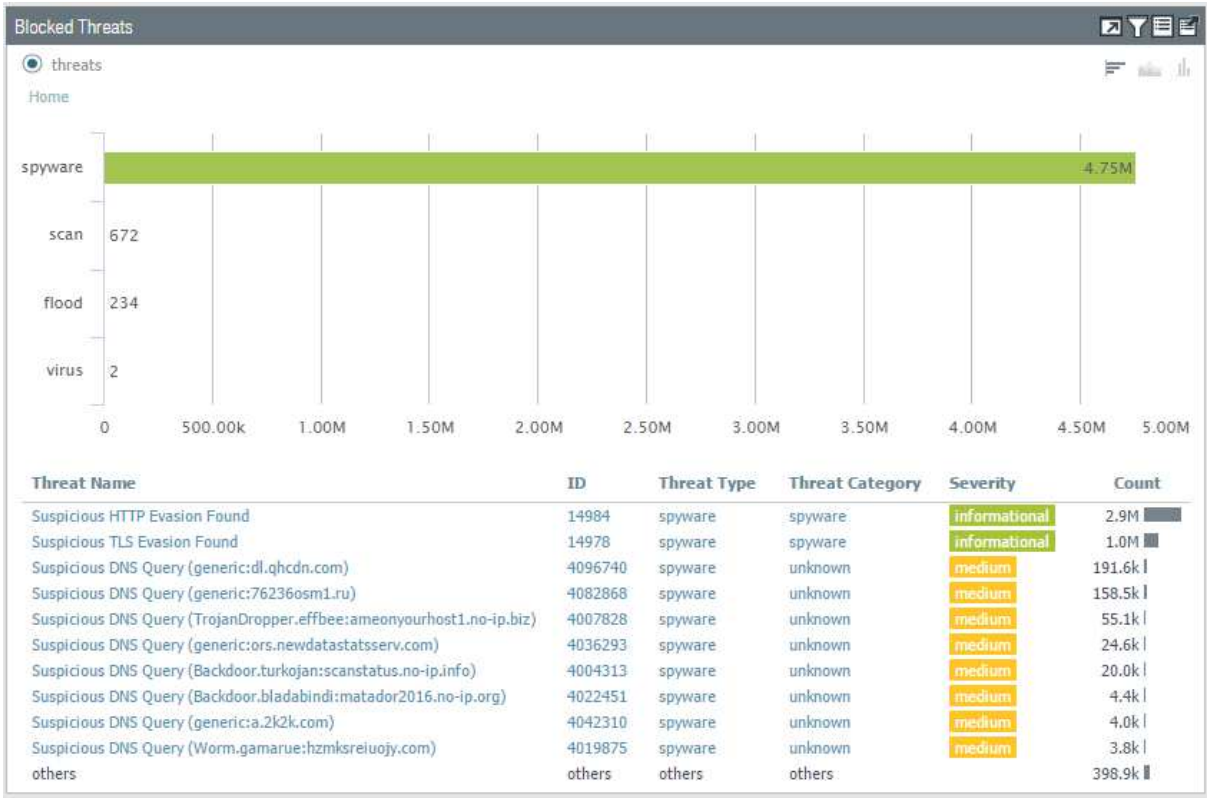
**Dropped Intrusion Events**

| Classification | Count |
|---|---|
| A Network Trojan was Detected | 613,343 |
| +2 Attempted Administrator Privilege Gain | 7,078 |
| +2 Web Application Attack | 6,362 |
| -2 Misc Activity | 1,779 |
| -2 Potential Corporate Policy Violation | 271 |
| +1 Attempted Information Leak | 204 |
| -1 Attempted User Privilege Gain | 131 |
| Attempted Denial of Service | 2 |

Last updated 2 minutes ago

- **การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Firewall** (ข้อมูล 1 เดือนย้อนหลัง)

  (ที่มา Paloalto:203.158.4.110)



**Blocked Threats**

threats

Home




| Threat Name | ID | Threat Type | Threat Category | Severity | Count |
|---|---|---|---|---|---|
| Suspicious HTTP Evasion Found | 14984 | spyware | spyware | informational | 2.9M |
| Suspicious TLS Evasion Found | 14978 | spyware | spyware | informational | 1.0M |
| Suspicious DNS Query (generic:dl.qhcdn.com) | 4096740 | spyware | unknown | medium | 191.6k |
| Suspicious DNS Query (generic:76236osm1.ru) | 4082868 | spyware | unknown | medium | 158.5k |
| Suspicious DNS Query (TrojanDropper.effbee:ameonyourhost1.no-ip.biz) | 4007828 | spyware | unknown | medium | 55.1k |
| Suspicious DNS Query (generic:ors.newdatastatsserv.com) | 4036293 | spyware | unknown | medium | 24.6k |
| Suspicious DNS Query (Backdoor.turkojan:scanstatus.no-ip.info) | 4004313 | spyware | unknown | medium | 20.0k |
| Suspicious DNS Query (Backdoor.bladabindi:matador2016.no-ip.org) | 4022451 | spyware | unknown | medium | 4.4k |
| Suspicious DNS Query (generic:a.2k2k.com) | 4042310 | spyware | unknown | medium | 4.0k |
| Suspicious DNS Query (Worm.gamarue:hzmksreiuojy.com) | 4019875 | spyware | unknown | medium | 3.8k |
| others | others | others | others | | 398.9k |