# รายงานการใช้งานระบบเครือข่ายคอมพิวเตอร์

## โครงสร้างพื้นฐานและระบบเครือข่าย ประจำเดือน พฤศจิกายน 66

- ระบบเครือข่ายคอมพิวเตอร์
- ระบบ Internet Data Center
- ระบบโทรคมนาคม

# สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

| | |
|---|---|
| 3 Nov 66 | เวลา 09.30 น. ระบบอินเตอร์เน็ต ที่สุรสัมนาคารใช้ไม่ได้ และได้ประสานงานกับเจ้าหน้าที่สุรสัมนาคาร ปัญหาเกิดจากระบบไฟฟ้าห้อง เครือข่าย trip เวลา 10.34 น. ระบบอินเตอร์เน็ตใช้ได้ |
| 7 Nov 66 | Access Point S5 หน้าห้อง 5317 มดเข้าเสียหาย |
| 8 Nov 66 | ตรวจสอบอาคาร F9 ห้อง 9103 ตรวจสอบพบภายในห้องมีอุปกรณ์เครือข่ายไร้สาย 1 ตัว และใกล้ทางเข้าห้องอีก 1 ตัว เพียงพอต่อการใช้งานภายในห้องเรียน |
| 8 Nov 66 | อาคารวิชาการ 2 ชั้น 1 ห้องเครือข่าย ห้องเก็บอุปกรณ์ระบบเครือข่ายแอร์เสีย ดำเนินการแจ้งซ่อมเรียบร้อย |
| 8 Nov 66 | หอพัก S4 ห้องเก็บอุปกรณ์ระบบเครือข่ายแอร์ไม่ทำงาน ดำเนินการแจ้งซ่อมเรียบร้อย |
| 9 Nov 66 | R7 ห้องเก็บอุปกรณ์ระบบเครือข่ายแอร์ไม่ทำงาน ดำเนินการแจ้งซ่อมเรียบร้อย |
| 11 Nov 66 | ตรวจสอบ Config อุปกรณ์เครือข่ายให้พร้อมใช้งาน ที่อาคาร F11 |

# สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

| | |
|---|---|
| 14 Nov 66 | ตรวจสอบ Config ห้อง Sever อาคารบรรณสาร |
| 14 Nov 66 | เปลี่ยนตำแหน่งติดตั้ง Access Point ที่สถานกีฬา |
| 17 Nov 66 | ดำเนินการตรวจสอบอาคารสัตว์ทดลอง พบว่าสายไฟเบอร์ขาดที่ระยะ 238 เมตร |
| 22 Nov 66 | สาย Fiber optic ขาด วัดจาก แอมฟิเทียเตอร์ ขาดที่ระยะ 198 m. ส่งผลให้ งานภูมิทัศน์ งาน ไทยศึกษานิทัศน์ สวนพฤษศาสตร์ ไม่สามารถใช้งาน internet |
| 22 Nov 66 | 6.30 น. หอพัก S1 ไฟฟ้าดับ ทำให้หอพัก และโซนส่วนอาคารเอนกประสงค์ใช้งานไม่ได้ตอนนี้ไฟฟ้ามาปกติ คาดว่า ups มีปัญหา |
| 28 Nov 66 | ตู้ Rack อาคารวิชาการ 2 มีเสียงเครื่องสำรองไฟฟ้าร้อง ดำเนินการตรวจสอบและแก้ไขเรียบร้อย |
| 30 Nov 66 | ตรวจสอบแนวสาย fiber optic ขาด จากการขุดทำรั้วเลี้ยงแพะ กับ แกะ |

# รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN)
# (ไม่รวมห้องปฏิบัติการคอมฯ)

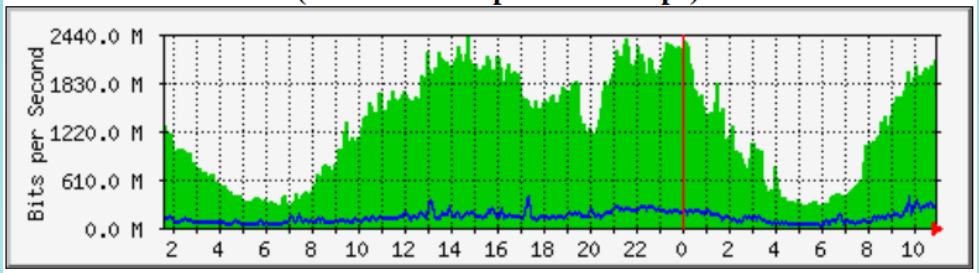
| วิธีการ | จำนวน |
|---|---|
| วิธีการแบบ ISE (802.1x) | 1,038 คน |

ที่มา (ise) https://203.158.4.207

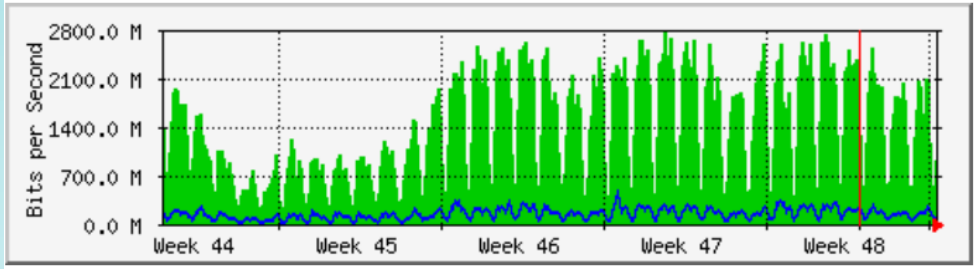
# รายงานการใช้งานระบบเครือข่าย

## Internet Gateway Traffic

**Link to True Internet (Domestic 6Gbps/Inter 3Gbps)**

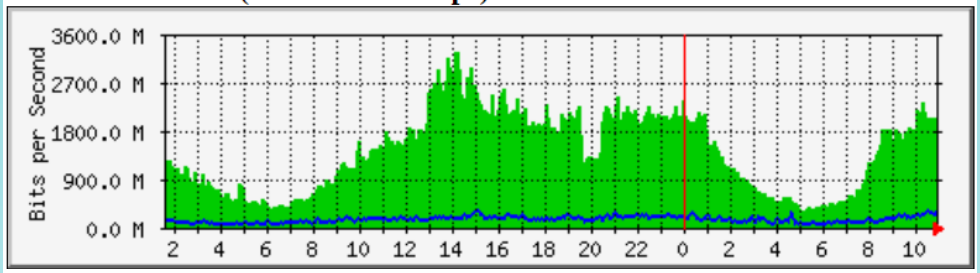



| | Max | Average | Current |
|---|---|---|---|
| In | 2417.1 Mb/s (24.2%) | 1258.4 Mb/s (12.6%) | 2103.3 Mb/s (21.0%) |
| Out | 378.3 Mb/s (3.8%) | 122.7 Mb/s (1.2%) | 271.4 Mb/s (2.7%) |

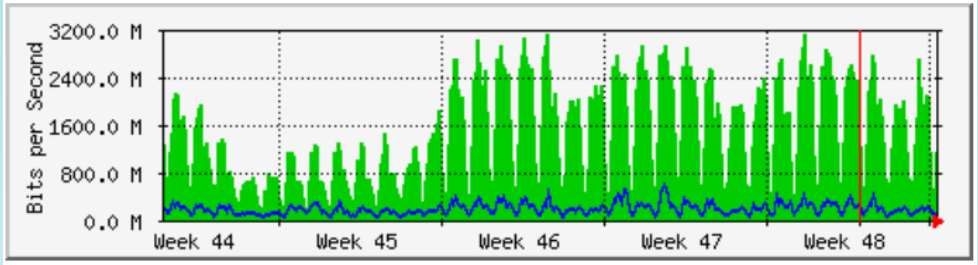



| | Max | Average | Current |
|---|---|---|---|
| In | 2797.2 Mb/s (28.0%) | 1349.0 Mb/s (13.5%) | 903.2 Mb/s (9.0%) |
| Out | 457.5 Mb/s (4.6%) | 133.7 Mb/s (1.3%) | 90.1 Mb/s (0.9%) |

**Link to UNINET (Domestic 10Gbps)**




| | Max | Average | Current |
|---|---|---|---|
| In | 3274.1 Mb/s (32.7%) | 1390.9 Mb/s (13.9%) | 2045.3 Mb/s (20.5%) |
| Out | 317.8 Mb/s (3.2%) | 139.8 Mb/s (1.4%) | 317.8 Mb/s (3.2%) |

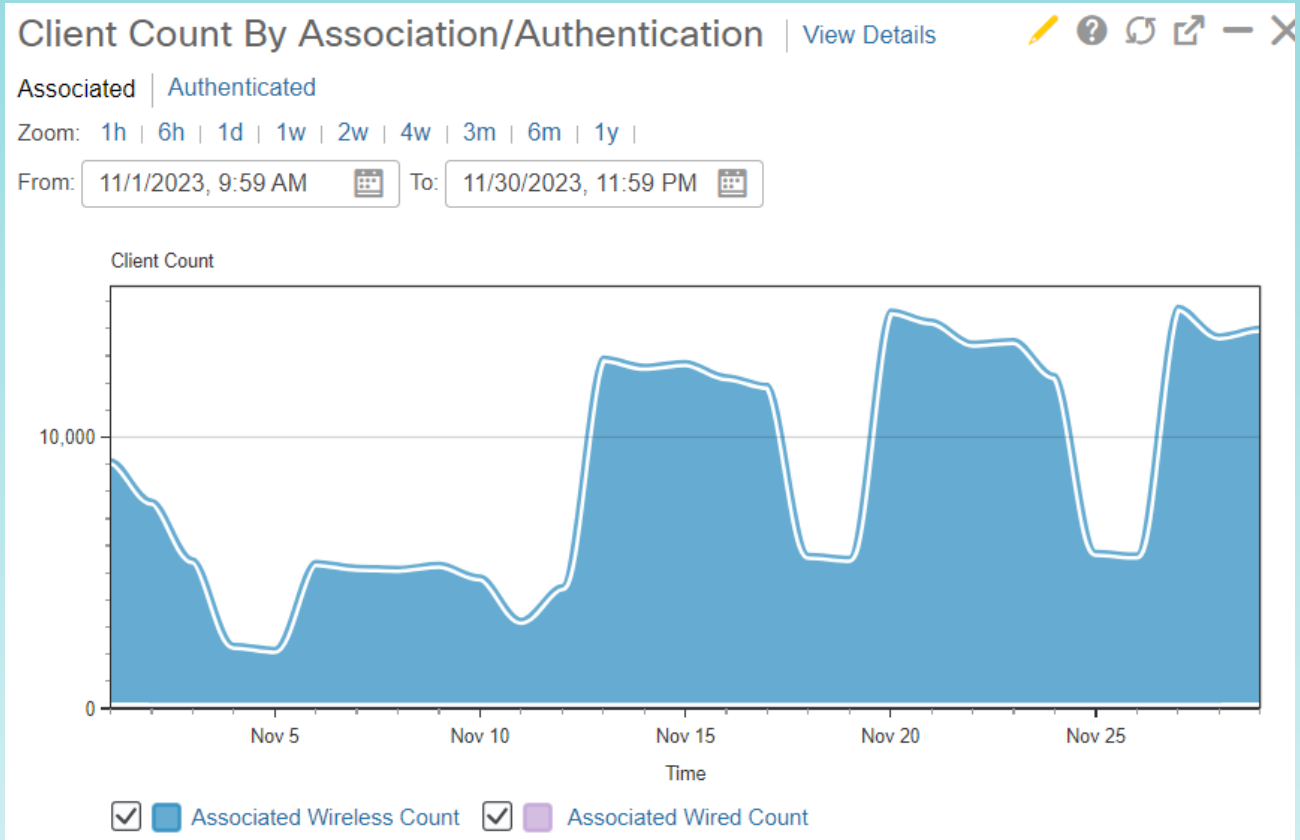



| | Max | Average | Current |
|---|---|---|---|
| In | 3132.6 Mb/s (31.3%) | 1419.3 Mb/s (14.2%) | 1142.7 Mb/s (11.4%) |
| Out | 582.6 Mb/s (5.8%) | 176.5 Mb/s (1.8%) | 115.4 Mb/s (1.2%) |

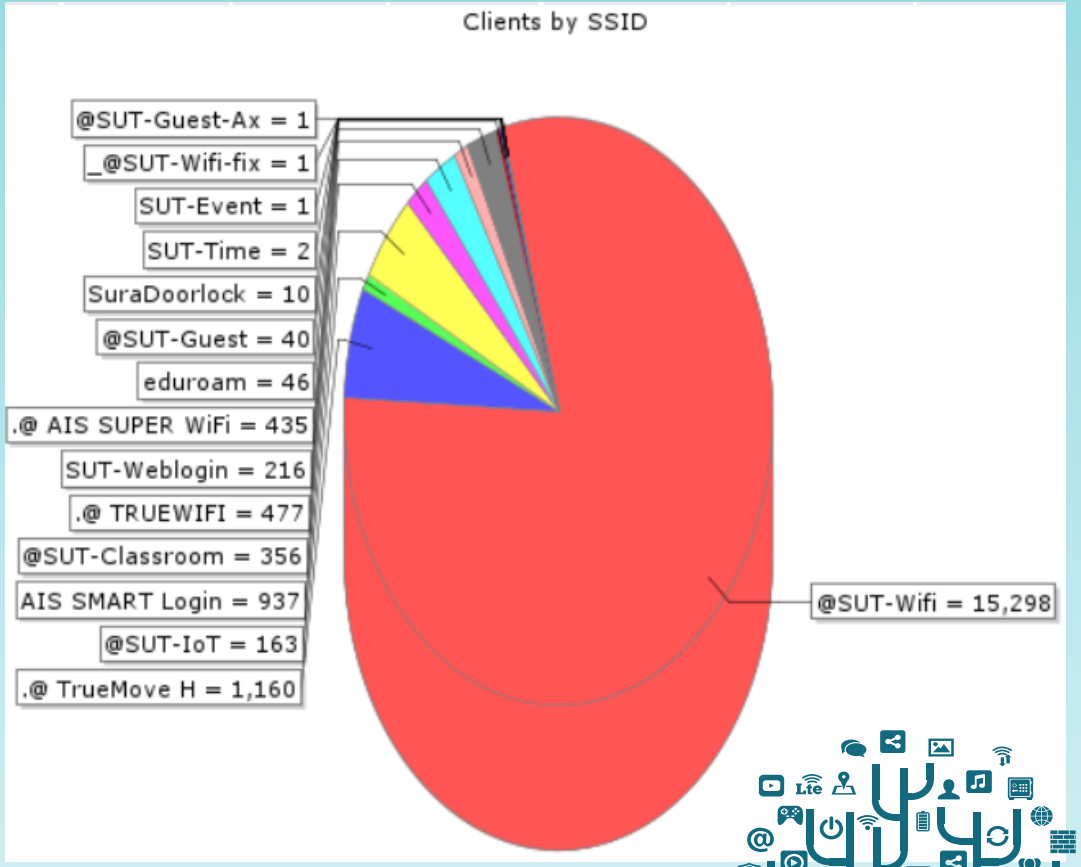
# รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่ายไร้สาย

## สรุปสถิติจำนวนผู้ใช้งานผ่านระบบ wireless ทั้งหมด

### สรุปปริมาณผู้ใช้งานต่อวัน




### แบ่งตาม SSID สถิติย้อนหลัง 1 เดือน




- ผู้ใช้งานผ่านระบบ wireless สูงสุด 14,821 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless, ต่ำสุด 2,202 คน/วัน
- ผู้ใช้งานผ่านระบบ wireless เฉลี่ย 8,863 คน/วัน

# สรุปการดำเนินการบนระบบ Internet Data Center

| | |
|---|---|
| 6 Nov 66 | ดำเนินการตรวจสอบ Server ของ อาจารย์ชิโนรัตน์ ไม่สามารถเข้าระบบ Server ที่เครื่องตั้งอยู่ที่โบรอนจากภายนอก มทส. ได้ อจ. ทดสอบเข้า Server เหล่านั้นจากเครื่องพีซีที่อยู่ในโบรอนสามารถเข้าได้ปกติ ระบบ Wifi ที่โบรอนสามารถใช้งานได้ปกติ 1. Policy Firewall ไม่มีการเปลี่ยนแปลงค่าอะไร 2. ทำการทดสอบตามรูป ip ใชนชุดของอาจารย์ สามารถเข้าได้จากข้างนอกปกติ นอกว่าที่แจ้ง ซึ่งเป็น policy เดียวกัน (routing ปกติ) จึงไม่ใช่เกิดจากระบบ Network หรือ Firewall |
| 7 Nov 66 | เวลา 21:44 น. ไฟฟ้าดับที่อาคารวิจัย gen 3 ตัวไม่ทำงาน ทั้งนี้ไม่กระทบต่อ IDC |
| 9 Nov 66 | ไฟฟ้าดับที่อาคารวิจัย gen ตัวไม่ทำงาน ทั้งนี้ไม่กระทบต่อ IDC |
| 30 Oct 66 | |

# สรุปการดำเนินการบนระบบโทรคมนาคม

8 Nov 66 เวลา 13.30 น. ประชุมหารือเรื่อง Flow การขอเบอร์โทรศัพท์ & การอัปเดตสมุดโทรศัพท์

# สรุปการดำเนินการอื่น ๆ

**16 Nov 66** ประชุมคณะกรรมการกำหนดร่างขอบเขตของงาน (Terms of Reference : TOR) งบประมาณ ประจำปี พ.ศ. 2567

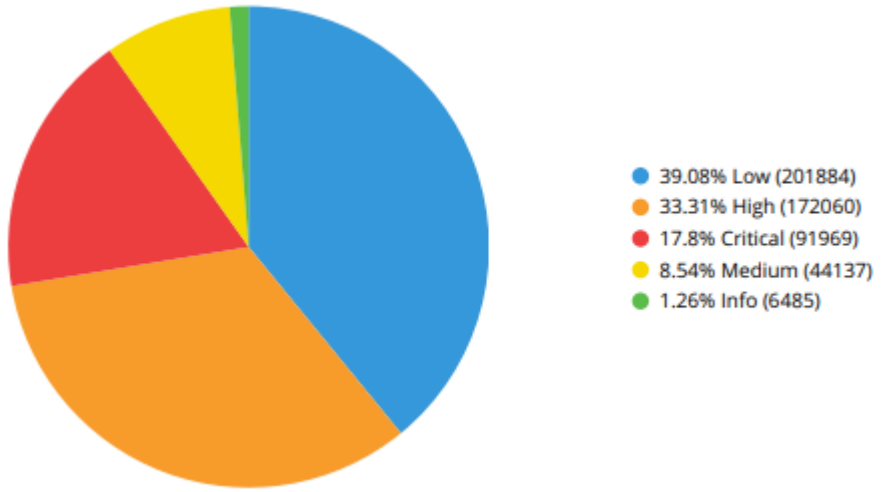
- จัดซื้ออุปกรณ์กระจายสัญญาณประจำเครือข่ายหลัก ดาต้าเซนเตอร์ และเครือข่ายย่อย จำนวน 1 ระบบ
- จัดเช่าอุปกรณ์เครือข่ายไร้สาย (Access Point) จำนวน 250 ชุด ตามโครงการพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย (Digital IT Infrastructure)
- จัดเช่าเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์ระบบปฏิบัติการเสมือน จำนวน 1 ระบบ
- จัดเช่าคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์ระบบปฏิบัติการเสมือน ตามโครงการพัฒนาระบบอินเตอร์เน็ตดาต้าเซนเตอร์ (Data Center) และศูนย์สำรองข้อมูล (DR-Site) จำนวน 1 ระบบ

**29 Nov 66** ประชุมคณะกรรมการร่างขอบเขตของงาน (Term of Reference : TOR) จัดจ้างบำรุงรักษาอุปกรณ์เครือข่าย และระบบบริหารจัดการ จำนวน 1 ระบบ

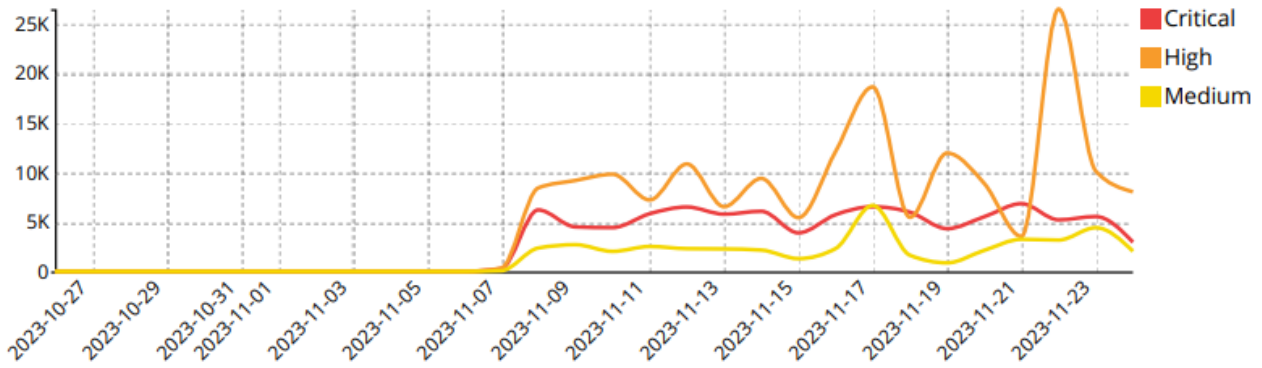
# ภัยคุกคามระบบเครือข่าย

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
## (ข้อมูล 1 เดือนย้อนหลัง)

### Intrusions By Severity




### Critical High and Medium Intrusions Timeline



# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
## (ข้อมูล 1 เดือนย้อนหลัง)

### Intrusions By Types

| # | Intrusion Type | Counts |
|---|---|---|
| 1 | Anomaly | 208,179 |
| 2 | SQL Injection | 66,129 |
| 3 | Code Injection | 42,348 |
| 4 | OS Command Injection | 36,462 |
| 5 | Malware | 23,913 |
| 6 | Other | 23,491 |
| 7 | Path Traversal | 19,755 |
| 8 | Buffer Errors | 13,849 |
| 9 | DoS | 9,901 |
| 10 | Permission/Priviledge/Access Control | 8,646 |
| 11 | XSS | 3,242 |
| 12 | Improper Authentication | 2,254 |
| 13 | Information Disclosure | 1,910 |
| 14 | Resource Management Errors | 32 |
| 15 | CSRF | 27 |
| 16 | Numeric Errors | 2 |

### Intrusions Detected Critical Severity Intrusions

| # | Attack Name | CVE-ID | Intrusion Type | Counts |
|---|---|---|---|---|
| 1 | PHPUnit.Eval-stdin.PHP.Remote.Code.Execution | CVE-2017-9841 | Code Injection | 33,256 |
| 2 | Andromeda.Botnet | | | 14,092 |
| 3 | Gh0st.Rat.Botnet | | | 6,701 |
| 4 | Bladabindi.Botnet | | | 6,193 |
| 5 | Zyxel.zhttpd.Webserver.Command.Injection | | OS Command Injection | 5,365 |
| 6 | Dasan.GPON.Remote.Code.Execution | CVE-2018-10561,CVE-2018-10562 | OS Command Injection | 3,470 |
| 7 | WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution | CVE-2017-8221,CVE-2017-8223, CVE-2017-8225,CVE-2017-18377 | Code Injection | 2,864 |
| 8 | Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection | CVE-2021-36260 | OS Command Injection | 2,759 |
| 9 | Zyxel.Firmware.error.message.Command.Injection | | | 1,736 |
| 10 | Java.Debug.Wire.Protocol.Insecure.Configuration | CVE-2017-6639 | Permission/Priviledge/Access Control | 1,325 |
| 11 | Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload | CVE-2017-11317,CVE-2017-11357,CVE-2019-18935 | Improper Authentication | 1,273 |
| 12 | Xtreme.RAT.Botnet | | | 1,176 |
| 13 | Realtek.SDK.UDPServer.Command.Execution | CVE-2021-35394 | OS Command Injection | 1,088 |
| 14 | TP-Link.Home.WiFi.Router.CGI.Referer.Authentication.Bypass | CVE-2018-11714,CVE-2018-12575 | Permission/Priviledge/Access Control | 937 |
| 15 | LB-LINK.goform.set_LimitClient_cfg.Command.Injection | CVE-2023-26801 | Code Injection | 915 |
| 16 | MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution | CVE-2015-1635 | Buffer Errors | 874 |
| 17 | Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass | | Improper Authentication | 873 |
| 18 | OpenSSL.Heartbleed.Attack | CVE-2014-0160 | Information Disclosure | 740 |
| 19 | D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution | CVE-2015-2051,CVE-2019-10891 | OS Command Injection | 651 |
| 20 | Joomla!.Core.Session.Remote.Code.Execution | CVE-2015-8562 | Code Injection | 468 |

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
## (ข้อมูล 1 เดือนย้อนหลัง)

### High Severity Intrusions

| # | Attack Name | CVE-ID | Intrusion Type | Counts |
|---|---|---|---|---|
| 1 | HTTP.URI.SQL.Injection | | SQL Injection | 65,566 |
| 2 | Multiple.Routers.GPON.form Login.Remote.Command.Injecti on | | OS Command Injection | 22,357 |
| 3 | Generic.XXE.Detection | CVE-2012-3363,CVE-2013-4295, CVE-2013-5015,CVE-2014-3490, CVE-2016-9563,CVE-2018-8527, CVE-2018-8532,CVE-2018-8533, CVE-2019-0537,CVE-2019-0948, CVE-2019-2647,CVE-2019-2648, CVE-2019-2649,CVE-2019-2650, CVE-2020-0765,CVE-2021-2400, CVE-2022-1018,CVE-2018-13415 ,CVE-2018-13416,CVE-2018-134 17,CVE-2018-15444,CVE-2018-1 8471,CVE-2019-17554,CVE-2019 -18227,CVE-2019-18227,CVE-20 20-15418,CVE-2020-15419,CVE- 2020-26981,CVE-2021-21658,CV E-2021-21659,CVE-2021-21672, CVE-2021-29447,CVE-2021-3120 7,CVE-2022-24463,CVE-2022-28 219,CVE-2022-43473,CVE-2022- 45468,CVE-2022-45876,CVE-202 2-46286,CVE-2022-46300 | Other | 16,474 |
| 4 | ALFA.TEaM.Web.Shell | | Malware | 15,381 |
| 5 | malicious-url | | | 13,087 |
| 6 | AndroxGh0st.Malware | | Malware | 8,211 |
| 7 | Mirai.Botnet | | | 8,096 |
| 8 | Web.Server.Password.File.Ac cess | | Permission/Priviledge/Access Control | 4,737 |
| 9 | SystemBC.Botnet | | | 4,099 |
| 10 | Linux.Kernel.TCP.SACK.Panic .DoS | CVE-2019-11477,CVE-2019-1147 8,CVE-2019-11479 | DoS | 3,419 |
| 11 | HTTP.Request.URI.Directory. Traversal | CVE-2001-0308,CVE-2011-0405, CVE-2018-7171,CVE-2018-10260 ,CVE-2018-11137,CVE-2018-162 88,CVE-2018-16836,CVE-2019-1 7662,CVE-2019-20085,CVE-2021 -40960,CVE-2021-42013 | Path Traversal | 2,308 |
| 12 | MS.IIS.FTP.IAC.Remote.Code. Execution | CVE-2010-3972 | Buffer Errors | 2,119 |
| 13 | TP-Link.Archer.AX21.Unauth enticated.Command.Injection | CVE-2023-1389 | Code Injection | 1,365 |
| 14 | MySQL.Login.Brute.Force | CVE-2012-2122 | Anomaly | 789 |
| 15 | RedLine.Stealer.Botnet | | | 381 |
| 16 | PHP.CGI.Argument.Injection | CVE-2012-1823,CVE-2012-2311, CVE-2012-2688 | Code Injection | 323 |
| 17 | FTP.Login.Brute.Force | | Anomaly | 316 |
| 18 | Adobe.XML.Entity.Injection | CVE-2009-3960 | Other | 271 |
| 19 | Joomla!.Component.HTTP.U RI.SQL.Injection | | SQL Injection | 246 |
| 20 | PhpStudy.Web.Server.Remot e.Code.Execution | | Code Injection | 196 |

### Medium Severity Intrusions

| # | Attack Name | CVE-ID | Intrusion Type | Counts |
|---|---|---|---|---|
| 1 | Apache.Solr.SolrResourceLoade r.Directory.Traversal | CVE-2013-6397 | Path Traversal | 15,848 |
| 2 | OpenSSL.DTLS.dtls1.buffer.reco rd.Function.DoS | CVE-2015-0206 | Buffer Errors | 10,758 |
| 3 | WordPress.xmlrpc.Pingback.Do S | | DoS | 6,349 |
| 4 | WordPress.xmlrpc.php.system. multicall.Amplification.Attack | | Anomaly | 3,935 |
| 5 | Cross.Site.Scripting | CVE-2007-1355,CVE-2007-6316, CVE-2008-2165,CVE-2008-3305, CVE-2008-3726,CVE-2008-4393, CVE-2008-4918,CVE-2009-1524, CVE-2010-2370,CVE-2010-3266, CVE-2010-4828,CVE-2011-0508, CVE-2011-0959,CVE-2011-0961, CVE-2011-1772,CVE-2011-2179, CVE-2011-2938,CVE-2011-3010, CVE-2011-3390,CVE-2011-4340, CVE-2016-3212,CVE-2016-9500, CVE-2018-2791,CVE-2018-5550, CVE-2018-8006,CVE-2018-17441 ,CVE-2018-17443 | XSS | 3,047 |
| 6 | TCP.Split.Handshake | | Anomaly | 775 |
| 7 | HTTP.GET.Request.Directory.Tra versal | CVE-2004-2112,CVE-2005-2020, CVE-2008-1145,CVE-2008-2938, CVE-2008-3727,CVE-2008-3938, CVE-2008-4243,CVE-2011-4714, CVE-2014-0780,CVE-2020-5410 | Path Traversal | 692 |
| 8 | PHP.Diescan | | Anomaly | 562 |
| 9 | LiteSpeed.Web.Server.NullByte.I nformation.Disclosure | CVE-2007-5654 | Information Disclosure | 488 |
| 10 | WordPress.REST.API.Username. Enumeration.Information.Disclo sure | CVE-2017-5487 | Information Disclosure | 366 |
| 11 | HTPasswd.Access | | Permission/Priviledge/Access Control | 192 |
| 12 | HTTP.URI.Script.XSS | CVE-2002-1315,CVE-2017-0068 | XSS | 192 |
| 13 | Apache.Axis2.Default.Password. Access | CVE-2010-0219 | Other | 111 |
| 14 | HTTP.Referer.Header.SQL.Injecti on | CVE-2007-1061 | SQL Injection | 107 |
| 15 | RealNetworks.Helix.Universal.Se rver.DoS | CVE-2004-0389 | DoS | 103 |
| 16 | Administrators.PWD | | Permission/Priviledge/Access Control | 99 |
| 17 | sqlmap.Scanner | | Anomaly | 76 |
| 18 | Phpweb.CMS.appcode.Informati on.Disclosure | | Information Disclosure | 49 |
| 19 | MS.IIS.WebDAV.Authentication. Bypass | CVE-2009-1535 | Improper Authentication | 48 |
| 20 | STUNSHELL.Web.Shell.Remote. Code.Execution | | Code Injection | 33 |

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
## (ข้อมูล 1 เดือนย้อนหลัง)

### Intrusion Victims

| # | Attack Victim | Counts | Critical | High | Medium | Percent of Total Attacks |
|---|---|---|---|---|---|---|
| 1 | 202.28.42.36 | 24,233 | | | | 20.16% |
| 2 | 203.158.6.2 | 22,581 | | | | 18.79% |
| 3 | 202.28.42.29 | 13,223 | | | | 11.00% |
| 4 | 10.0.63.49 | 10,434 | | | | 8.68% |
| 5 | 203.158.6.27 | 8,765 | | | | 7.29% |
| 6 | 202.28.42.71 | 4,080 | | | | 3.39% |
| 7 | 203.158.7.1 | 4,064 | | | | 3.38% |
| 8 | 202.28.42.25 | 3,880 | | | | 3.23% |
| 9 | 203.158.7.45 | 3,841 | | | | 3.20% |
| 10 | 202.28.42.38 | 3,330 | | | | 2.77% |
| 11 | 192.168.31.131 | 3,093 | | | | 2.57% |
| 12 | 34.80.59.191 | 3,052 | | | | 2.54% |
| 13 | 203.158.6.88 | 2,645 | | | | 2.20% |
| 14 | 10.1.176.78 | 2,548 | | | | 2.12% |
| 15 | 192.168.160.56 | 2,217 | | | | 1.84% |
| 16 | 203.158.4.100 | 2,163 | | | | 1.80% |
| 17 | 172.67.168.62 | 1,816 | | | | 1.51% |
| 18 | 104.21.26.69 | 1,733 | | | | 1.44% |
| 19 | 203.158.4.80 | 1,382 | | | | 1.15% |
| 20 | 203.158.7.71 | 1,112 | | | | 0.93% |

### Intrusion Sources

| # | Attack Source | Counts | Critical | High | Medium | Percent of Total Attacks |
|---|---|---|---|---|---|---|
| 1 | 83.97.73.87 | 64,507 | | | | 34.55% |
| 2 | 20.150.219.203 | 20,931 | | | | 11.21% |
| 3 | 184.105.192.2 | 12,961 | | | | 6.94% |
| 4 | 51.79.230.42 | 9,299 | | | | 4.98% |
| 5 | 66.240.205.34 | 8,993 | | | | 4.82% |
| 6 | 94.130.164.87 | 7,702 | | | | 4.13% |
| 7 | 200.85.194.146 | 6,625 | | | | 3.55% |
| 8 | 102.129.153.241 | 6,277 | | | | 3.36% |
| 9 | 183.89.167.173 | 5,505 | | | | 2.95% |
| 10 | 103.207.166.64 | 5,397 | | | | 2.89% |
| 11 | 84.54.51.111 | 5,241 | | | | 2.81% |
| 12 | 80.82.78.39 | 4,432 | | | | 2.37% |
| 13 | 84.54.51.66 | 3,987 | | | | 2.14% |
| 14 | 45.95.146.97 | 3,794 | | | | 2.03% |
| 15 | 203.158.1.34 | 3,794 | | | | 2.03% |
| 16 | 65.108.129.48 | 3,716 | | | | 1.99% |
| 17 | 92.205.190.232 | 3,450 | | | | 1.85% |
| 18 | 20.199.64.162 | 3,418 | | | | 1.83% |
| 19 | 131.159.24.205 | 3,391 | | | | 1.82% |
| 20 | 156.226.21.79 | 3,264 | | | | 1.75% |

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet
## (ข้อมูล 1 เดือนย้อนหลัง)

Intrusions Blocked

| # | Intrusion Name | Intrusion Type | Severity | Counts |
|---|---|---|---|---|
| 1 | PHPUnit.Eval-stdin.PHP.Remote.Code.Execution | Code Injection | Critical | 33,256 |
| 2 | Andromeda.Botnet | | Critical | 14,092 |
| 3 | Gh0st.Rat.Botnet | | Critical | 6,701 |
| 4 | Bladabindi.Botnet | | Critical | 6,193 |
| 5 | Zyxel.zhttpd.Webserver.Command.Injection | OS Command Injection | Critical | 5,365 |
| 6 | Dasan.GPON.Remote.Code.Execution | OS Command Injection | Critical | 3,470 |
| 7 | WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution | Code Injection | Critical | 2,864 |
| 8 | Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection | OS Command Injection | Critical | 2,759 |
| 9 | Zyxel.Firmware.error.message.Command.Injection | | Critical | 1,736 |
| 10 | Java.Debug.Wire.Protocol.Insecure.Configuration | Permission/Priviledge/Access Control | Critical | 1,325 |
| 11 | Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload | Improper Authentication | Critical | 1,273 |
| 12 | Xtreme.RAT.Botnet | | Critical | 1,176 |
| 13 | Realtek.SDK.UDPServer.Command.Execution | OS Command Injection | Critical | 1,088 |
| 14 | TP-Link.Home.WiFi.Router.CGI.Referer.Authentication.Bypass | Permission/Priviledge/Access Control | Critical | 937 |
| 15 | LB-LINK.goform.set_LimitClient_cfg.Command.Injection | Code Injection | Critical | 915 |
| 16 | MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution | Buffer Errors | Critical | 874 |
| 17 | Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass | Improper Authentication | Critical | 873 |
| 18 | OpenSSL.Heartbleed.Attack | Information Disclosure | Critical | 740 |
| 19 | D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution | OS Command Injection | Critical | 651 |
| 20 | Joomla!.Core.Session.Remote.Code.Execution | Code Injection | Critical | 468 |

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet สำหรับโซน REG และ Finance

## Top Applications by Bandwidth

| # | Application | Bandwidth | Sent | Received |
|---|---|---|---|---|
| 1 | HTTPS.BROWSER | | | 239.76 GB |
| 2 | YouTube | | | 100.02 GB |
| 3 | HTTP.BROWSER | | | 98.78 GB |
| 4 | Facebook | | | 81.90 GB |
| 5 | tcp/21064 | | | 64.95 GB |
| 6 | Oracle.TNS | | | 41.65 GB |
| 7 | DTLS | | | 37.47 GB |
| 8 | Apple.iPhone | | | 34.70 GB |
| 9 | SSL | | | 34.42 GB |
| 10 | Microsoft.Windows.Update | | | 33.97 GB |

## Top Applications by Sessions

| # | Application | Sessions |
|---|---|---|
| 1 | HTTPS.BROWSER | 2,061,099 |
| 2 | DNS | 1,445,818 |
| 3 | HTTP.BROWSER | 968,177 |
| 4 | HTTP | 373,650 |
| 5 | SSL | 348,555 |
| 6 | Endpoint Control Registration | 341,814 |
| 7 | Microsoft.Portal | 300,221 |
| 8 | udp/5353 | 285,677 |
| 9 | DTLS | 249,131 |
| 10 | netbios forward | 235,132 |

# การยับยั้งการโจมตีบนระบบเครือข่าย โดย อุปกรณ์ Next Gen Firewall : Fortinet สำหรับโซน REG และ Finance

## Intrusions Detected

| # | Attack Name | Severity | CVE-ID | Counts |
|---|---|---|---|---|
| 1 | malicious-url | High | | 4 |

## Events by Severity