

# รายงานการใช้งาน ระบบเครือข่ายคอมพิวเตอร์ ประจำเดือน พ.ค. 2569

ฝ่ายโครงสร้างพื้นฐานและระบบเครือข่าย



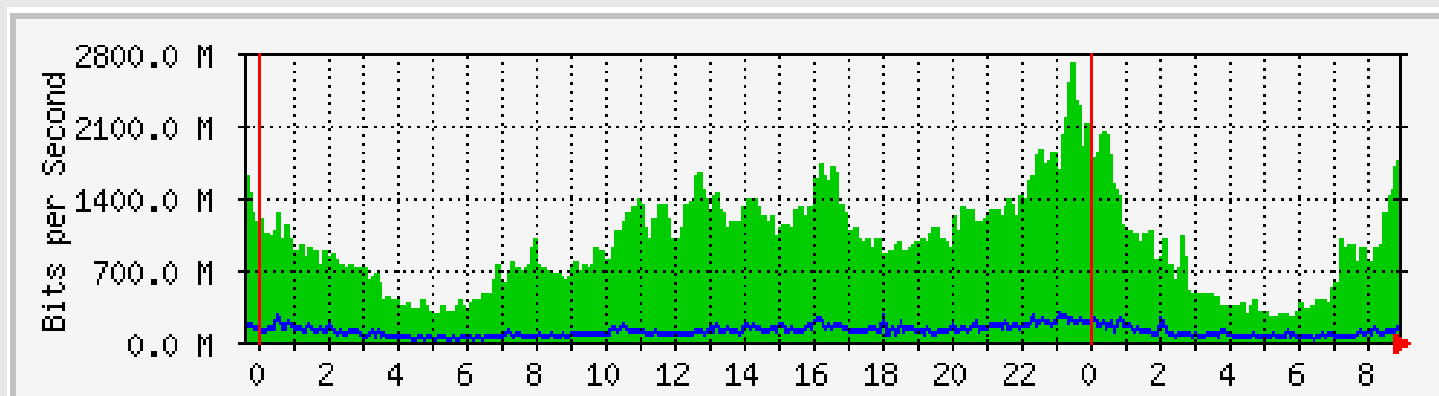
# รายงานจำนวนผู้ใช้งานผ่านระบบเครือข่าย (LAN) (ไม่รวมห้องปฏิบัติการคอมพิวเตอร์)

วิธีการ	จำนวน
วิธีการแบบ ISE (802.1x)	301 คน

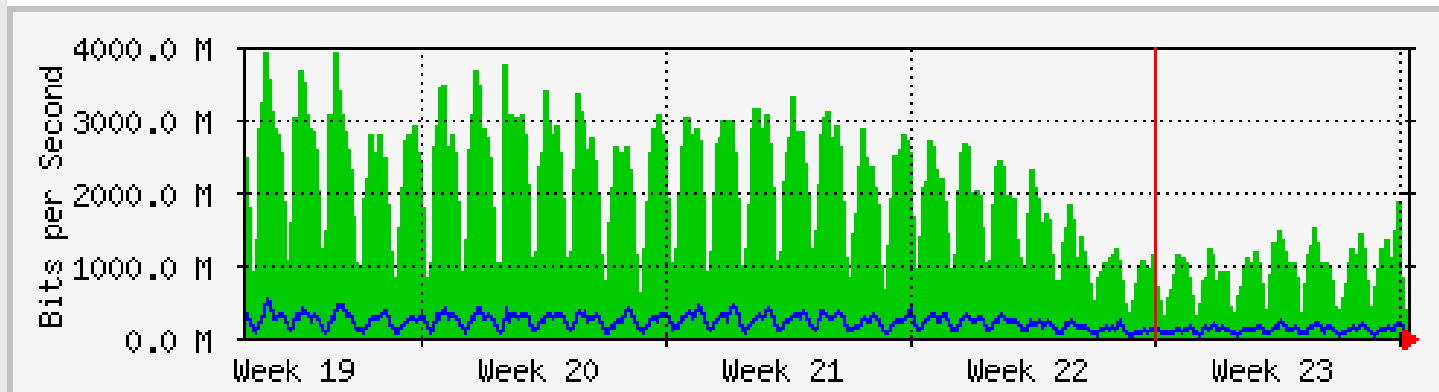
# รายงานการใช้งานระบบเครือข่าย

## Internet Gateway Traffic

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

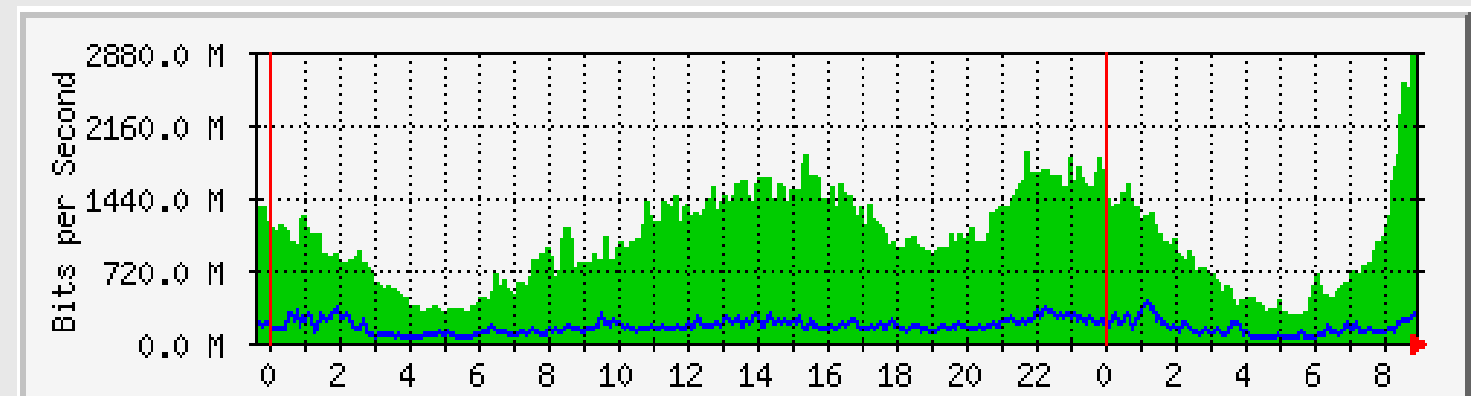


	Max	Average	Current
<b>In</b>	2702.6 Mb/s (27.0%)	933.6 Mb/s (9.3%)	1743.7 Mb/s (17.4%)
<b>Out</b>	256.1 Mb/s (2.6%)	95.2 Mb/s (1.0%)	133.0 Mb/s (1.3%)

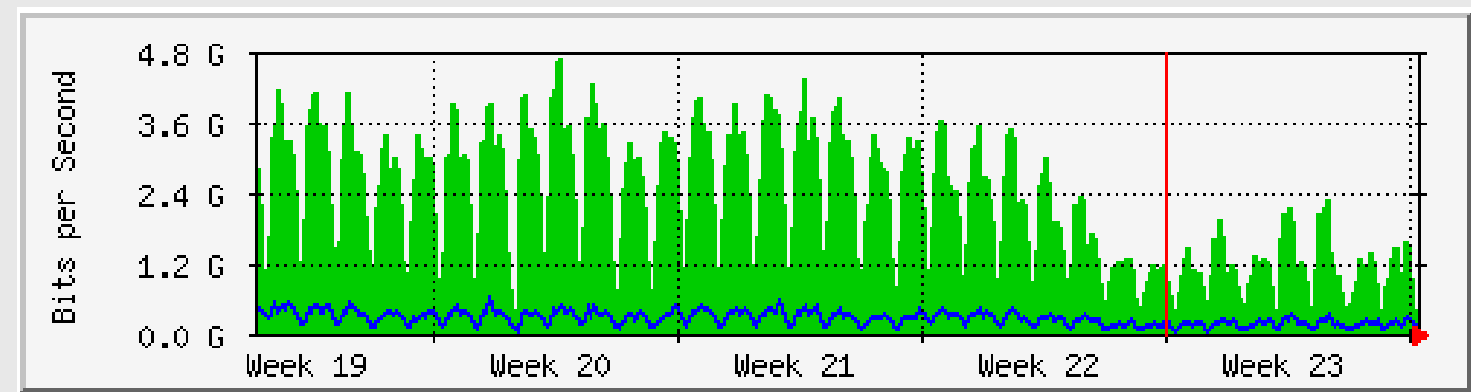


	Max	Average	Current
<b>In</b>	3910.9 Mb/s (39.1%)	1731.8 Mb/s (17.3%)	310.0 Mb/s (3.1%)
<b>Out</b>	481.8 Mb/s (4.8%)	185.9 Mb/s (1.9%)	47.2 Mb/s (0.5%)

### Link to UNINET (Domestic 10Gbps)



	Max	Average	Current
<b>In</b>	2850.6 Mb/s (28.5%)	1005.9 Mb/s (10.1%)	2696.8 Mb/s (27.0%)
<b>Out</b>	379.0 Mb/s (3.8%)	149.8 Mb/s (1.5%)	255.1 Mb/s (2.6%)



	Max	Average	Current
<b>In</b>	4686.9 Mb/s (46.9%)	2109.7 Mb/s (21.1%)	416.9 Mb/s (4.2%)
<b>Out</b>	612.2 Mb/s (6.1%)	243.0 Mb/s (2.4%)	76.6 Mb/s (0.8%)

# สรุปการดำเนินการบนระบบเครือข่ายคอมพิวเตอร์

หัวข้อ	จำนวน (งาน)
ซ่อมแซมอุปกรณ์ Network (ผลกระทบในระดับอาคาร)	-
งานสำรวจหน้างาน ประมาณราคาการจัดจ้าง ขยาย/ปรับปรุง/ซ่อมแซม/บำรุงรักษาระบบ	11
การ Monitor/Standby ระบบ Network	11
ติดตั้ง/ซ่อมแซม สายสัญญาณ Network	18
งานให้คำแนะนำปรึกษาแก่ผู้ใช้บริการ	4

# สรุปการดำเนินการบนระบบ INTERNET DATA CENTER

หัวข้อ	จำนวน (งาน)
ติดตั้งอุปกรณ์ Data Center (ผลกระทบในระดับมหาวิทยาลัย)	-
บริหารจัดการระบบ Data Center	3
บริหารจัดการระบบ Network และ Security	15
จัดสรร VS/VM, Web	3
การ Monitor/Standby ระบบ Data Center	10
บริหารจัดการ Email Account / บริหารจัดการ Wifi Account / บริหารจัดการ G.dot Account	24
ตรวจสอบ/ปรับปรุงแก้ไข ด้านความปลอดภัยระบบสารสนเทศ	-

# สรุปการดำเนินการบนระบบโทรคมนาคม

หัวข้อ	จำนวน (งาน)
แก้ไขอุปกรณ์ Telephone (ผลกระทบในระดับอาคาร)	1
การ Monitor/Standby ระบบ Telephone	1
ติดตั้ง/ซ่อมแซม สายสัญญาณ Telephone	20
จัดสรรหมายเลข/IP Phone/Soft Phone	1
กำกับดูแลการติดตั้ง เภมคีน อุปกรณ์/ครุภัณฑ์ และเอกสารประกอบที่เกี่ยวข้องให้ถูกต้องแล้ว เสร็จภายในเวลาที่กำหนด	-

## สรุปการดำเนินงานด้านอื่น ๆ

หัวข้อ	จำนวน (งาน)
เข้าร่วมประชุม/เข้าร่วมกิจกรรมต่างๆของมหาวิทยาลัย	8
จัดการรายงานการประชุม /แจ้งเวียนรับรองรายงาน /แจ้งสรุปมติกับผู้ที่เกี่ยวข้องภายในระยะเวลาที่กำหนด	1
จัดทำเอกสารใบขอให้อัดซื้อ จัดจ้าง รวบรวมรายละเอียดต่าง ๆ ได้ถูกต้องครบถ้วน และบริหารจัดการส่งให้ส่วนพัสดุได้ทันตามกำหนด	2
จัดทำไฟล์นำเสนองานรูปแบบ PPT ออกแบบไฟล์สื่อประชาสัมพันธ์ รูปแบบ PDF, PNG ที่เกี่ยวข้องกับการกิจของฝ่าย/หน่วยงาน	1
รวบรวมข้อมูลและจัดทำกรอบค่างบประมาณประจำปีในภาพรวมของหน่วยงาน	2
สรุปรายงานผลการดำเนินงานของหน่วยงานประจำเดือน/ประจำไตรมาส และรายงานต่อคณะกรรมการของมหาวิทยาลัย หรือระบบออนไลน์	1
ร่างหนังสือแบบที่มีเนื้อหาลักษณะเฉพาะพิเศษ	1
ร่างหนังสือแบบฟอร์มพื้นฐานทั่วไป	2

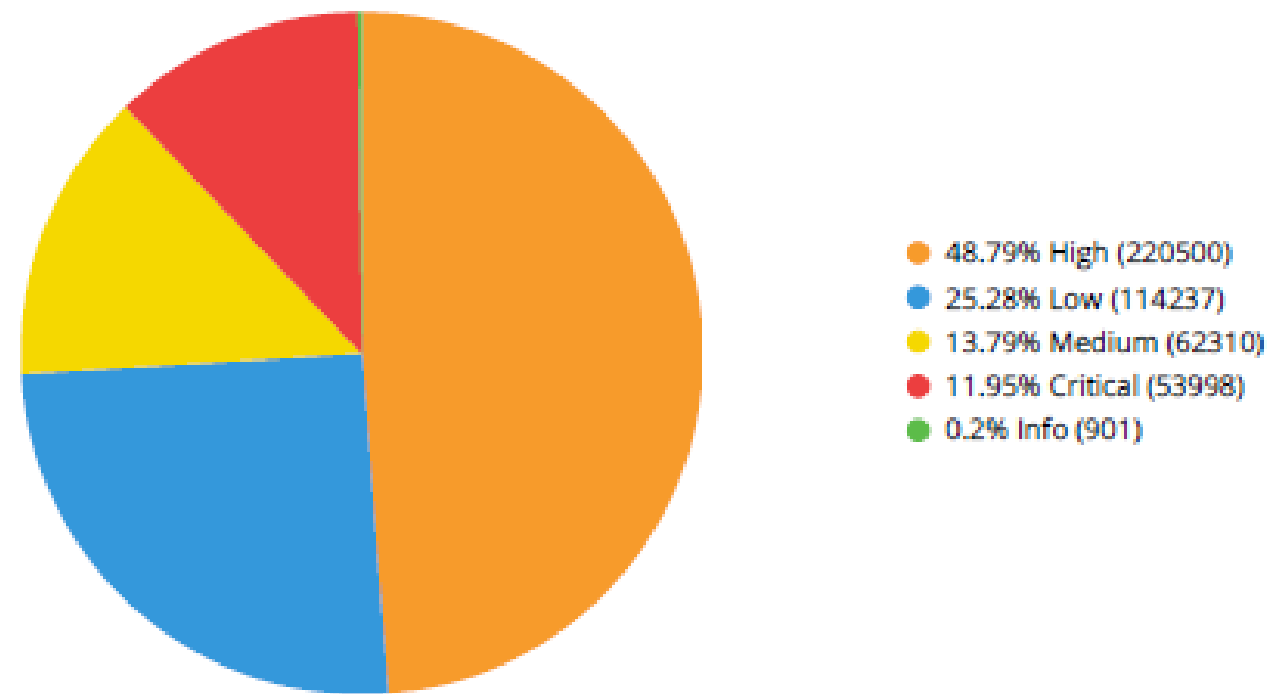
# ภัยคุกคามระบบเครือข่าย



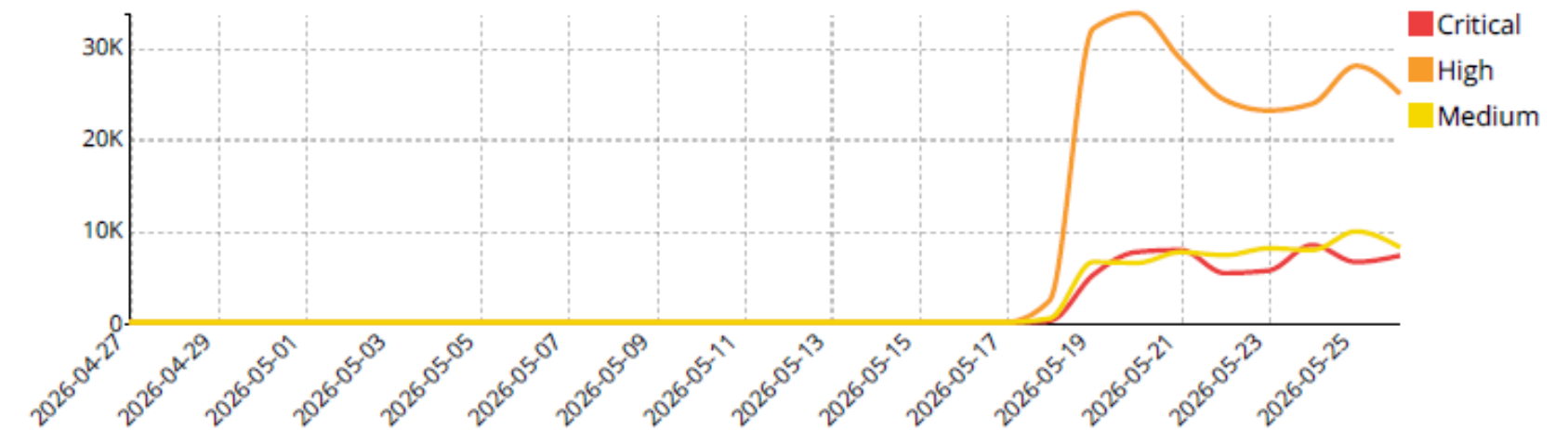
# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

## SUT Gateway of IPS Report

Intrusions By Severity



Critical High and Medium Intrusions Timeline



# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

## SUT Gateway of IPS Report

### Intrusion Victims



#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	202.28.42.26				35,048	19.40%
2	117.18.127.179				23,034	12.75%
3	172.67.161.65				18,206	10.08%
4	172.67.157.210				18,202	10.08%
5	172.67.175.87				18,191	10.07%
6	172.67.199.217				18,187	10.07%
7	202.28.42.36				12,348	6.84%
8	203.158.5.129				10,126	5.61%
9	202.28.42.40				3,954	2.19%
10	44.244.22.128				3,313	1.83%
11	202.28.42.23				2,800	1.55%
12	203.158.3.112				2,665	1.48%
13	49.228.131.165				2,404	1.33%
14	203.158.3.129				2,129	1.18%
15	104.21.95.156				2,052	1.14%
16	172.67.145.177				2,048	1.13%
17	203.158.4.150				1,670	0.92%
18	203.158.3.49				1,435	0.79%
19	203.158.3.131				1,430	0.79%
20	203.158.7.5				1,395	0.77%

### Intrusion Sources



#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	203.158.7.23				72,786	29.50%
2	79.124.40.174				42,711	17.31%
3	194.233.77.183				34,656	14.04%
4	10.1.143.32				15,244	6.18%
5	10.0.187.99				11,476	4.65%
6	144.172.92.68				9,289	3.76%
7	193.32.162.28				8,856	3.59%
8	5.61.209.126				8,594	3.48%
9	10.1.173.157				7,764	3.15%
10	36.95.143.31				6,645	2.69%
11	10.0.53.36				4,525	1.83%
12	176.65.139.254				3,975	1.61%
13	221.159.119.6				3,751	1.52%
14	193.32.162.104				3,073	1.25%
15	162.62.213.150				2,755	1.12%
16	10.0.52.210				2,404	0.97%
17	211.37.177.87				2,396	0.97%
18	176.65.148.183				1,998	0.81%
19	123.234.81.180				1,972	0.80%
20	176.65.139.140				1,881	0.76%

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



Intrusions Blocked

## SUT Gateway of IPS Report

#	Intrusion Name	Intrusion Type	Severity	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	18,423
2	Hikvision.Products.SDK.WebLanguage.Tag.Command.Injection	OS Command Injection	Critical	10,007
3	Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	Other	Critical	2,969
4	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	2,809
5	Amadey.Botnet		Critical	2,417
6	njRAT.Botnet		Critical	2,404
7	Cisco.IOS.XE.Web.UI.Unauthorized.Account.Creation	Permission/Privilege/Access Control	Critical	2,132
8	DZS.GPON.Remote.Code.Execution	OS Command Injection	Critical	1,811
9	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	1,716
10	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	1,481
11	PHP.Filters.Chain.Remote.Code.Execution	Anomaly	Critical	1,348
12	TOTOLINK.Devices.tecgi.Command.Injection	OS Command Injection	Critical	917
13	PTZOptics.PT30X.param.Authentication.Bypass	Improper Authentication	Critical	879
14	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	Critical	834
15	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	721
16	Java.Debug.Wire.Protocol.Insecure.Configuration	Permission/Privilege/Access Control	Critical	690
17	Tenda.Devices.formSetMacFilterCfg.Buffer.Overflow	Buffer Errors	Critical	475
18	Ralink.SDK.goform.SystemCommand.Command.Injection	Code Injection	Critical	387
19	Babar		Critical	379
20	D-Link.DIR.Devices.Session.Cookie.Buffer.Overflow	Buffer Errors	Critical	222

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet

## SUT Gateway Cyber Threat Assessment

High Risk Applications



High Risk Applications

No matching log data for this report

Top Application Vulnerability Exploits Detected



Top Application Vulnerability Exploits Detected

No matching log data for this report

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet



Web Usage : Top Web Applications

Top Web Applications

No matching log data for this report

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สำหรับ REG และ Finance

## FIN-REG Security Analysis

Top Applications by Bandwidth



Top Applications by Bandwidth

No matching log data for this report

Top Applications by Sessions



Top Applications by Sessions

No matching log data for this report

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สำหรับ REG และ Finance

## FIN-REG Security Analysis

Intrusions Detected



Events by Severity



Intrusions Detected

No matching log data for this report

Events by Severity

No matching log data for this report

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สำหรับ REG และ Finance

FIN-REG Cyber Threat Assessment

Security and Threat Prevention  
High Risk Applications



Top Application Vulnerability Exploits Detected

## High Risk Applications

No matching log data for this report

## Top Application Vulnerability Exploits Detected

No matching log data for this report

# การยับยั้งการโจมตีบนระบบเครือข่าย โดยอุปกรณ์ Next Gen Firewall : Fortinet สำหรับ REG และ Finance

FIN-REG Cyber Threat Assessment



Top Web Applications

Top Web Applications

No matching log data for this report