

๗. บุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุด

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งานอินเทอร์เน็ตของกรมฯ พบบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุด ดังนี้

ลำดับที่	ผู้ใช้งาน	หน่วยงาน	User Name	Data Transferred
๑	OMA4	ศสท.	๑๐.๑๐.๑๐.๒๓๖	๙๑๒ GB
๒	อังสุมาลิน โสภเชือก	กบช.	aungsumalin_coep	๕๔ GB
๓	สุทธิลักษณ์ ระวีวรรณ	รองอธิบดี	suthiluckw_dp๑	๒๘ GB
๔	อภิวัฒน์ สุขรักษา	สสอ.	apiwat_pr	๒๑ GB
๕	ทวีพร น้อยสะอาด	สลก.	Taweeporn_sec	๒๐ GB
๖	สิริกอร์ วิชาลวณิชชัย	สสอ.	sirikorn_pr	๒๐ GB
๗	จตุรงค์ โทบุรี	สปล.	Jaturong_mg	๑๘ GB
๘	เสาวภา กิ่งวงษา	สสอ.	saowapa_pr	๑๗ GB
๙	Forti Analyze	Forti Analyze	๒๐.๒๐.๒๐.๒๔๘	๑๗ GB
๑๐	ชาตรี ฤกษ์	หน้าห้อง ผชช.	CHATREE_spl๑	๑๗ GB

ภาพแสดงบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุด จากระบบ

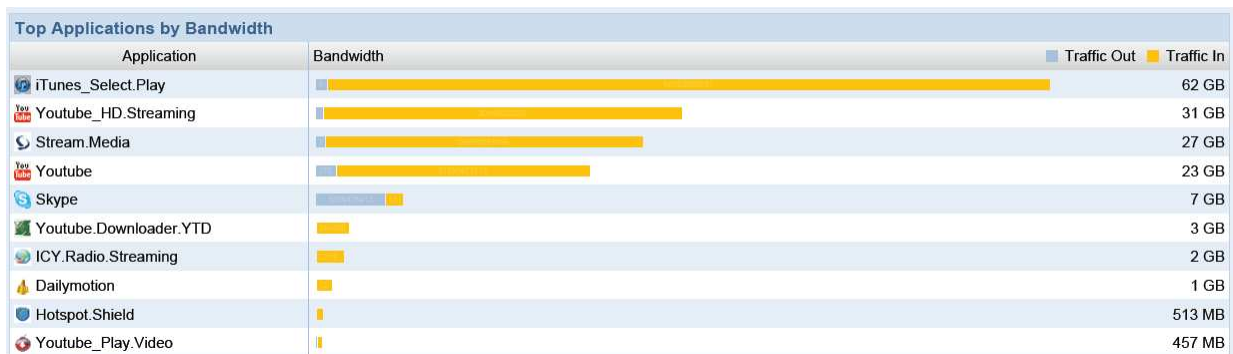
DMCR-User Top 10 Users by Bandwidth	
User	Bandwidth
10.10.10.236	912 GB
aungsumalin_coep	54 GB
suthiluckw_dp1	28 GB
apiwat_pr	21 GB
Taweeporn_sec	20 GB
sirikorn_pr	20 GB
Jaturong_mg	18 GB
saowapa_pr	17 GB
20.20.20.248	17 GB
CHATREE_spl1	17 GB

๘. Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งาน Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับที่	Application	Bandwidth
๑	iTunes_Select.Play	๖๒ GB
๒	Youtube_HD.Streaming	๓๑ GB
๓	Stream.Media	๒๗ GB
๔	Youtube	๒๓ GB
๕	Skype	๘ GB
๖	Youtube.Downloader.YTD	๗ GB
๗	ICY.Radio.Streaming	๓ GB
๘	Dailymotion	๒ GB
๙	Hotspot.Shield	๑ GB
๑๐	Youtube_Play.Video	๕๑๓ MB

ภาพแสดง Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

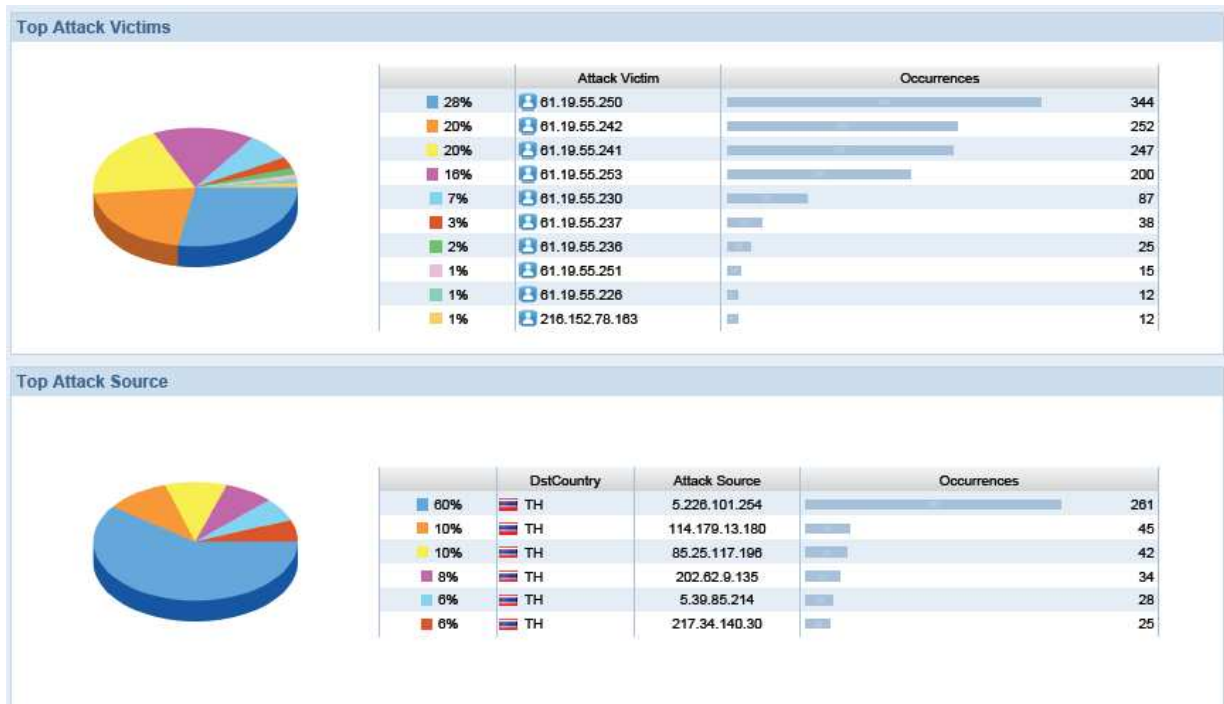


๙. เครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงเครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับ ดังนี้

ลำดับที่	Name	IP Address	จำนวน
๑	Web Km	๖๑.๑๙.๕๕.๒๕๐	๓๔๔
๒	Web_Dmcr	๖๑.๑๙.๕๕.๒๔๒	๒๕๒
๓	Authen	๖๑.๑๙.๕๕.๒๔๑	๒๔๗
๔	Web Omcrc	๖๑.๑๙.๕๕.๒๕๓	๒๐๐
๕	Complaint	๖๑.๑๙.๕๕.๒๓๐	๘๗
๖	marinegiscenter	๖๑.๑๙.๕๕.๒๓๗	๓๘
๗	Oma๔	๖๑.๑๙.๕๕.๒๓๖	๒๕
๘	Omcm Server	๖๑.๑๙.๕๕.๒๕๑	๑๕
๙	Panda	๖๑.๑๙.๕๕.๒๒๖	๑๒
๑๐	DPIS	๒๑๖.๑๕๒.๗๘.๑๖๓	๑๒

ภาพแสดง เครื่องคอมพิวเตอร์ที่ถูกบุกรุกมากที่สุด ๑๐ อันดับ



๑๐. รูปแบบการโจมตีผ่านอินเทอร์เน็ต

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรูปแบบการโจมตีผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับ ที่	Name	จำนวน
๑	Joomla.JCE.Extension.Remote.File.Upload	๙๖๒
๒	phpMyAdmin.Remote.Code.Execution	๒๗๓
๓	udp_flood	๒๖๕
๔	PHP.CGI.Argument.Injection	๒๐๗
๕	ZmEu.Vulnerability.Scanner	๑๐๖
๖	Open.Flash.Chart.PHP.File.Upload	๕๗
๗	MS.Windows.ASN.๑.Bitstring.Heap.Overflow	๓๗
๘	MS.RPC.DCOM.ObjectActivationInterface.BufferOverflow.CMD	๓๖
๙	HTTP.URI.SQL.Injection	๒๙
๑๐	HTTP.URI.SQL.Injection	๒๗

Top Attacks	
Threat Name	Counts
Joomla.JCE.Extension.Remote.File.Upload	962
phpMyAdmin.Remote.Code.Execution	273
udp_flood	265
PHP.CGI.Argument.Injection	207
ZmEu.Vulnerability.Scanner	106
Open.Flash.Chart.PHP.File.Upload	57
MS.Windows.ASN.1.Bitstring.Heap.Overflow	37
MS.RPC.DCOM.ObjectActivationInterface.BufferOverflow.CMD	36
HTTP.Chunk.Overflow	29
HTTP.URI.SQL.Injection	27
SoftiaCom.WMailserver.Buffer.Overflow	23
FTP.USER.Command.Overflow	14
udp_src_session	5
udp_dst_session	4
Fiesta.Exploit.Kit	4
Backdoor.Infection.Redirection	2
Mozilla.Firefox.Chrome.Page.Loading.Restriction.Bypass	2
OpenSSL.ClientMasterkey.Overflow	2
Admin.Php.Upload	2
Wordpress.MM.Forms.Community.Plugin.Arbitrary.File.Upload	1