๗. บุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุด

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งานอินเตอร์เน็ตของกรมฯ พบบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุด ดังนี้

ลำดับที่	ผู้ใช้งาน	หน่วยงาน	User Name	Data Transfered
๑	DPIS	DPIS	DPIS	๕๕๖ GB
๒	สุธาทิพย์ ขำดี	นิติการ	suthathip_law	๒๕ GB
๓	ทัศนีย์ เทพศิริ	สปล.	thudsanee_mg	๒๒ GB
๔	ภาสินี พัฒน์บรมย์	นิติการ	pasinee_law	๒๑ GB
๕	นายธนา ยิ่งเจริญ	กผง.	DHANA_PN	๒๐ GB
๖	นายไพรัตน์ เจริญศิริ	สสอ.	pairath_pr	๒๐ GB
๗	ว่าที่ร้อยตรีฐปพน อำนายสมบัติ	นิติการ	Dhapapon_law	๑๙ GB
๘	ณัฐพล บุญยืน	ศสท.กผง.	natapon_it	๑๙ GB
๙	วาสนา แก้วขาว	สลก.	wassana_sec	๑๗ GB
๑๐	Forti Analyzer	Forti Analyzer	Forti Analyzer	๑๗ GB

ภาพแสดงบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุด จากระบบ

DMCR-User Top 10 Users by Bandwidth

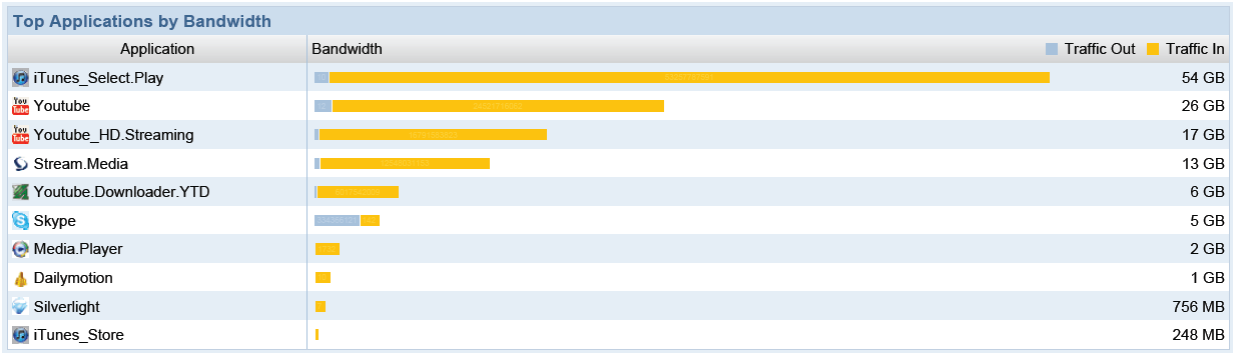
User	Bandwidth
10.10.10.231	556 GB
suthathip_law	25 GB
thudsanee_mg	22 GB
pasinee_law	21 GB
DHANA_PN	20 GB
pairath_pr	20 GB
Dhapapon_law	19 GB
natapon_it	19 GB
wassana_sec	17 GB
20.20.20.248	17 GB

๘. Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งาน Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับที่	Application	Bandwidth
๑	iTunes_Select.Play	๕๔ GB
๒	Youtube	๒๖ GB
๓	Youtube_HD.Streaming	๑๗ GB
๔	Stream.Media	๑๓ GB
๕	Youtube.Downloader.YTD	๖ GB
๖	Skype	๕ GB
๗	Media.Player	๒ GB
๘	Dailymotion	๑ GB
๙	Silverlight	๗๕๖ MB
๑๐	iTunes_Store	๒๔๘ MB

ภาพแสดง Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

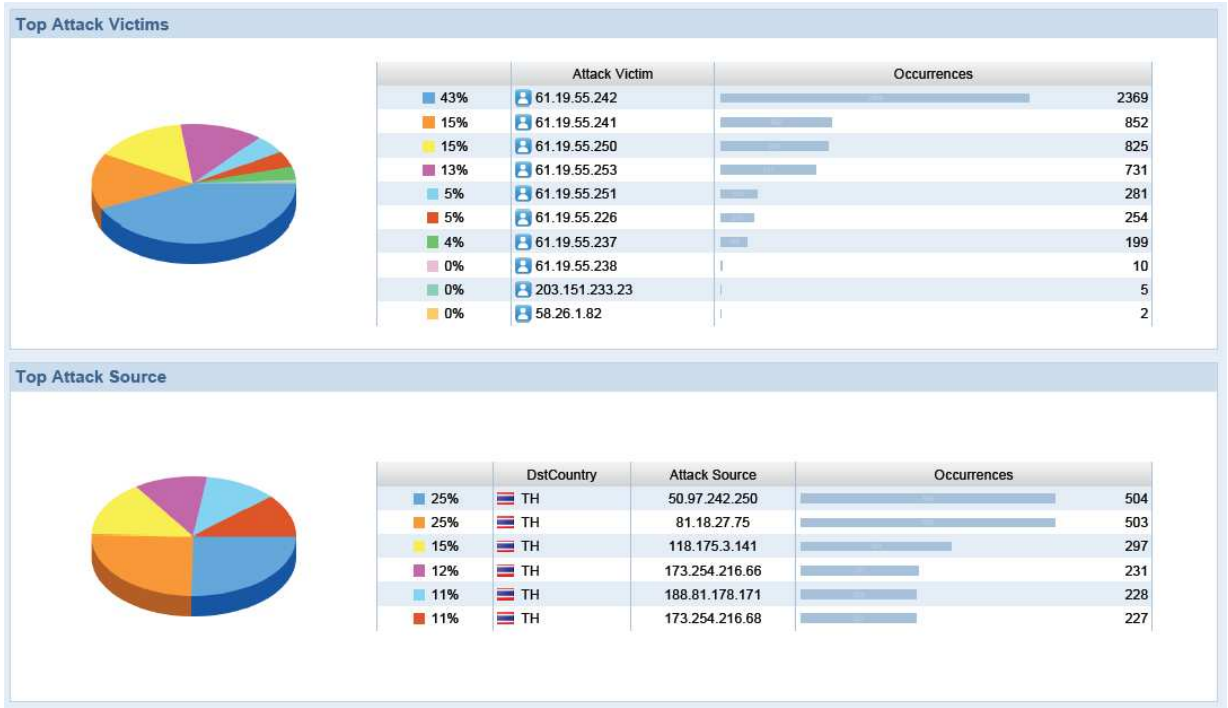


๙. เครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเตอร์เน็ตมากที่สุด

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงเครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเตอร์เน็ตมากที่สุด ดังนี้

ลำดับที่	Name	IP Address	จำนวน
๑	Web_Dmcr	๖๑.๑๙.๕๕.๒๔๒	๒,๓๖๙
๒	Authen	๖๑.๑๙.๕๕.๒๔๑	๘๕๒
๓	Web Km	๖๑.๑๙.๕๕.๒๕๐	๘๒๕
๔	Web Omcrc	๖๑.๑๙.๕๕.๒๕๓	๗๓๑
๕	Omcm Server	๖๑.๑๙.๕๕.๒๕๑	๒๘๑
๖	Panda	๖๑.๑๙.๕๕.๒๒๖	๒๕๔
๗	Database๑/๑	๖๑.๑๙.๕๕.๒๓๗	๑๙๙
๘	Database๑/๒	๖๑.๑๙.๕๕.๒๓๘	๑๐
	๒๐๓.๑๕๑.๒๓๓.๓๑	๒๐๓.๑๕๑.๒๓๓.๒๓	๕
		๕๘.๒๖.๑.๖๒	๒

ภาพแสดง เครื่องคอมพิวเตอร์ที่ถูกบุกรุกมากที่สุด ๑๐ อันดับ



๑๐. รูปแบบการโจมตีผ่านอินเตอร์เน็ต

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรูปแบบการโจมตีผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับที่	Name	จำนวน
๑	HTTP.URI.SQL.Injection	๑,๙๐๘
๒	ZmEu.Vulnerability.Scanner	๑,๕๓๘
๓	Joomla.JCE.Extension.Remote.File.Upload	๑,๑๐๔
๔	PHP.CGI.Argument.Injection	๗๗๑
๕	phpMyAdmin.Remote.Code.Execution	๖๘๓
๖	Open.Flash.Chart.PHP.File.Upload	๓๐๒
๗	DLink.IP.Cameras.rtpd.cgi.OS.Command.Injection	๕๔
๘	MS.Windows.ASN.๑.Bitstring.Heap.Overflow	๓๑
๙	MS.RPC.DCOM.ObjectActivationInterface.BufferOverflow.CMD	๒๐
๑๐	HTTP.Chunk.Overflow	๑๓

ภาพแสดง รูปแบบการโจมตีผ่านอินเตอร์เน็ต

Top Attacks

Threat Name	Counts
HTTP.URI.SQL.Injection	1908
ZmEu.Vulnerability.Scanner	1538
Joomla.JCE.Extension.Remote.File.Upload	1104
PHP.CGI.Argument.Injection	771
phpMyAdmin.Remote.Code.Execution	683
Open.Flash.Chart.PHP.File.Upload	302
DLink.IP.Cameras.rtpd.cgi.OS.Command.Injection	54
MS.Windows.ASN.1.Bitstring.Heap.Overflow	31
MS.RPC.DCOM.ObjectActivationInterface.BufferOverflow.CMD	20
HTTP.Chunk.Overflow	13
WordPress.OptimizePress.Theme.Arbitrary.File.Upload	10
Wordpress.wpStoreCart.Plugin.Arbitrary.File.Upload	10
HTTP.URI.Script.XSS	8
udp_flood	6
WordPress.Plugin.Advanced.Custom.Fields.Remote.File.Inclusion	6
Wordpress.MM.Forms.Community.Plugin.Arbitrary.File.Upload	4
WordPress.Property.Plugin.Arbitrary.File.Upload	4
FTP.Text.Line.Too.Long	3
MailEnable.WebMail.Authentication.Buffer.Overflow	2
Fiesta.Exploit.Kit	1