ที่ อย ๐๐๑๙/ว ๑๐๒๑๙

ศาลากลางจังหวัดพระนครศรีอยุธยา
ถนนสายเอเชีย อย ๑๓๐๐๐

๑๙ มิถุนายน ๒๕๖๓

เรื่อง การโจมตีของโปรแกรมทำลายระบบเครื่องคอมพิวเตอร์ลูกข่าย (Clients)

เรียน นายอำเภอทุกอำเภอ

สิ่งที่ส่งมาด้วย ข้อมูลโปรแกรมทำลายระบบคอมพิวเตอร์ฯ จำนวน ๑ ชุด

ด้วยกรมการพัฒนาชุมชน แจ้งว่าได้ตรวจสอบการโจมตีของโปรแกรมทำลายระบบเครื่องคอมพิวเตอร์ลูกข่าย (Clients) ด้วยโปรแกรม ESET Remote Administrator Console ประจำเดือนพฤษภาคม ๒๕๖๓ พบว่าเครื่องคอมพิวเตอร์ในความรับผิดชอบของหน่วยงานส่วนภูมิภาค ถูกไวรัสโจมตี รายละเอียดตามสิ่งที่ส่งมาด้วย

ในการนี้ เพื่อให้การใช้งานเครื่องคอมพิวเตอร์ลูกข่ายเป็นไปอย่างมีประสิทธิภาพ จึงให้อำเภอมอบหมายสำนักงานพัฒนาชุมชนอำเภอ แจ้งเจ้าหน้าที่ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสำนักงานพัฒนาชุมชนอำเภอ ดำเนินการ ดังนี้

๑. เปิดเครื่องคอมพิวเตอร์เพื่อให้โปรแกรมป้องกันไวรัสอัปเดต (Update) และระบบจะทำการสแกนไวรัสอัตโนมัติทุกวัน เวลา ๑๒.๐๐ น.

๒. หลีกเลี่ยงการดาวน์โหลดไฟล์และติดตั้งโปรแกรมที่ไม่จำเป็นต่อการปฏิบัติงาน หรือการเข้าใช้งานเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม และเว็บไซต์ที่ผิดกฎหมาย

๓. ก่อนหรือระหว่างเปิดเว็บไซต์หากมีข้อความแจ้งเตือน “เว็บไซต์ข้างหน้ามีมัลแวร์” หรือโปรแกรมป้องกันไวรัสมีข้อความแจ้งเตือน ให้ทำความเข้าใจกับข้อความดังกล่าว หากไม่แน่ใจไม่ควรเปิดเว็บไซต์ดังกล่าว

๔. ศึกษาคำอธิบายโปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีเครื่องคอมพิวเตอร์ลูกข่าย ประจำเดือนพฤษภาคม ๒๕๖๓ เพื่อเป็นแนวทางป้องกันการถูกโจมตี

จึงเรียนมาเพื่อพิจารณาดำเนินการ

ขอแสดงความนับถือ

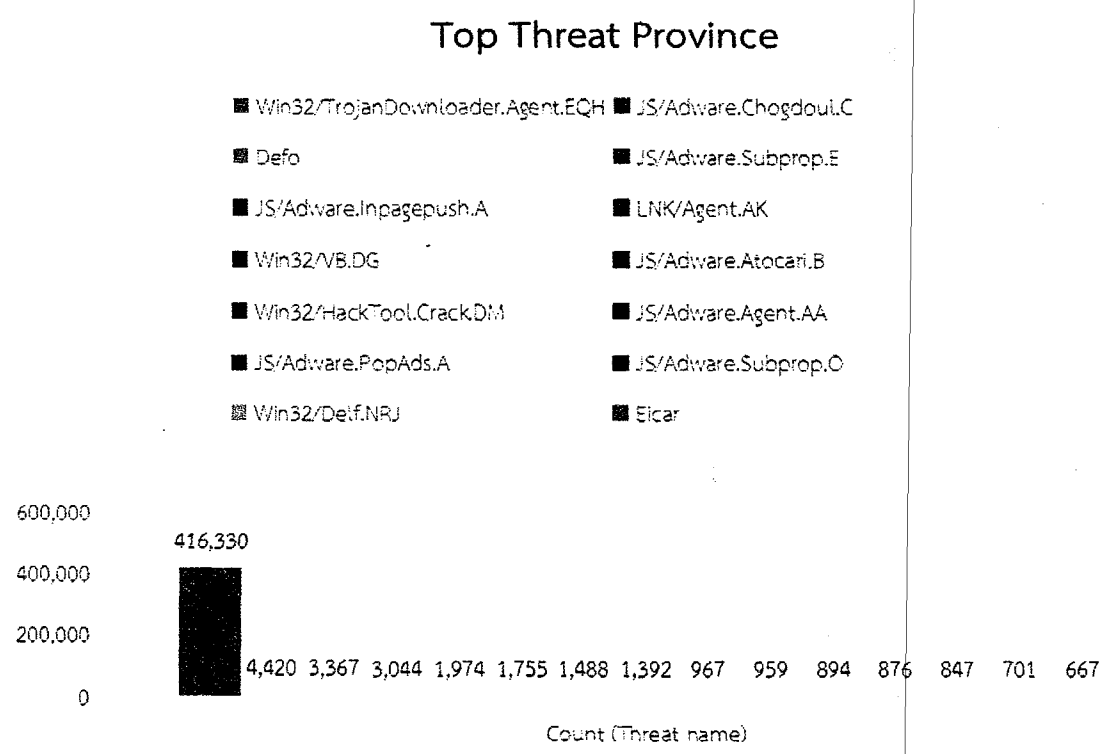
(นายกิจจา ทองแดง)
พัฒนาการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดพระนครศรีอยุธยา

สำนักงานพัฒนาชุมชนจังหวัด
กลุ่มงานสารสนเทศการพัฒนาชุมชน
โทร.๐๓๕-๓๓๖๕๔๒
โทรสาร.๐๓๕-๓๓๖๕๔๑
Mail:cddayutthaya@gmail.com
สุทธิมาศ ใบบัวทอง โทร.๐๘ ๕๘๐๓ ๗๑๖๒

พฤษภาคม ๒๕๖๓

ตารางที่ ๑ โปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีเครื่องคอมพิวเตอร์ลูกข่ายหน่วยงานส่วนภูมิภาค

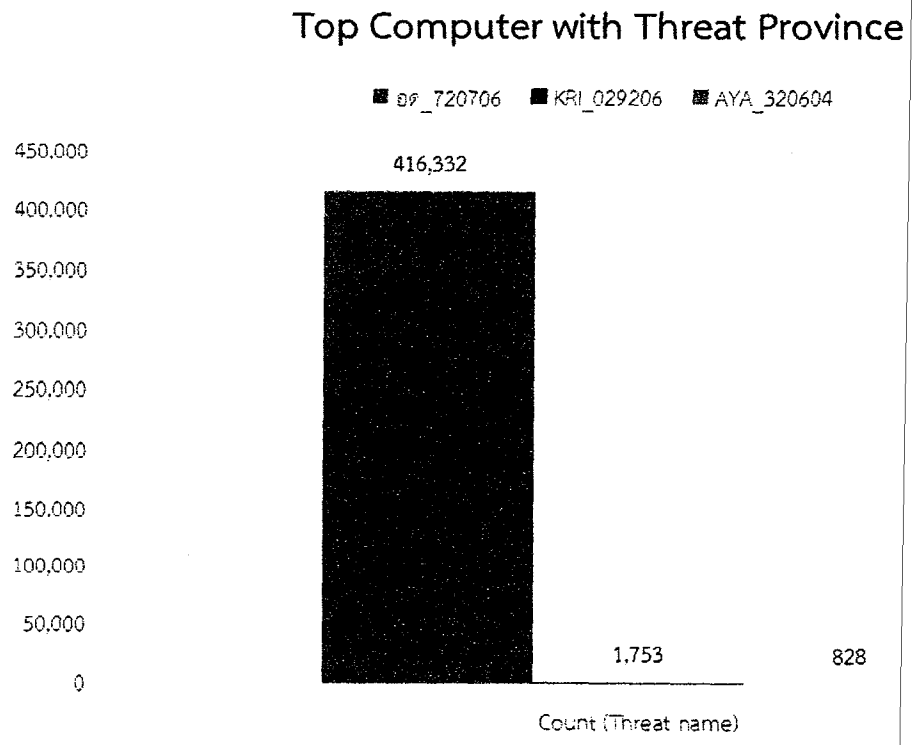
ลำดับที่	โปรแกรมทำลายระบบคอมพิวเตอร์	จำนวนครั้ง	ร้อยละ
1	Win32/TrojanDownloader.Agent.EQH	416,330	94.69
2	JS/Adware.Chogdoul.C	4,420	1.01
3	Defo	3,367	0.77
4	JS/Adware.Subprop.E	3,044	0.69
5	JS/Adware.Inpagepush.A	1,974	0.45
6	LNK/Agent.AK	1,755	0.40
7	Win32/VB.DG	1,488	0.34
8	JS/Adware.Atocari.B	1,392	0.32
9	Win32/HackTool.Crack.DM	967	0.22
10	JS/Adware.Agent.AA	959	0.22
11	JS/Adware.PopAds.A	894	0.20
12	JS/Adware.Subprop.O	876	0.20
13	Win32/Delf.NRJ	847	0.19
14	Eicar	701	0.16
15	Win32/Brontok.B	667	0.15
	รวมทั้งหมด	439,681	100



พฤษภาคม ๒๕๖๓

ตารางที่ ๒ เครื่องคอมพิวเตอร์ลูกข่ายส่วนภูมิภาคที่ไวรัสโจมตี

ลำดับที่	ชื่อเครื่องคอมพิวเตอร์	จำนวนครั้ง
1	อด_720706	416,332
2	KRI_029206	1,753
3	AYA_320604	828



ตารางที่ ๓ คำอธิบายโปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีเครื่องคอมพิวเตอร์ลูกข่าย ส่วนภูมิภาค ประจำเดือนพฤษภาคม 2563

เครื่องคอมพิวเตอร์ลูกข่ายชื่อ อด_720706 (จังหวัดอุดรธานี)

โปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีมากที่สุด	การโจมตี	สาเหตุ	ผลกระทบ
Win32/TrojanDownloader.Agent.EQH	แฝงตัวเข้าไปในแอปพลิเคชันที่ถูกดาวน์โหลด	การดาวน์โหลดหรือติดตั้งแอปพลิเคชันที่ไม่พึงประสงค์จำพวกฟรีแวร์	แอปพลิเคชันที่ถูกดาวน์โหลดและติดตั้งนั้น อาจจะเข้ามาล้วงข้อมูลความลับของผู้ใช้งาน

เครื่องคอมพิวเตอร์ลูกข่ายชื่อ KRI_029206 (จังหวัดกาญจนบุรี)

โปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีมากที่สุด	การโจมตี	สาเหตุ	ผลกระทบ
LNK/Agent.AK	กระทำซ้ำแฟ้มงาน และซ่อนไฟล์งานของผู้ใช้งานโดยเปลี่ยนชื่อเป็นภาษาหรืออักขระที่อ่านไม่ออก	การใช้งานแฟรชไดร์ฟหรือการแชร์ไฟล์จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง โดยไม่มีการสแกนไวรัส หรือโปรแกรมป้องกันไวรัสในเครื่อง	ทำให้ไฟล์งานของผู้ใช้งานมีหลายไฟล์ ซึ่งอาจจะเป็นไฟล์เปล่า หรือ Shortcut

เครื่องคอมพิวเตอร์ลูกข่ายชื่อ AYA_320604 (จังหวัดพระนครศรีอยุธยา)

โปรแกรมทำลายระบบคอมพิวเตอร์ที่โจมตีมากที่สุด	การโจมตี	สาเหตุ	ผลกระทบ
Win32/Delf.NRJ	แฝงตัวมากับระบบปฏิบัติการที่ผิดกฎหมายหรือไม่น่าเชื่อถือ	ดาวน์โหลด ติดตั้งระบบปฏิบัติการที่ไม่มีลิขสิทธิ์หรือผิดกฎหมาย	เวลาเข้าเว็บไซต์ต่าง ๆ จะลิงค์ไปอีกที่หนึ่ง ส่งผลให้เกิดความรำคาญ และในระยะยาวอาจจะทำให้คอมพิวเตอร์ของผู้ใช้งานมีอาการเข้าเว็บอื่น ๆ ที่ไม่ประสงค์โดยอัตโนมัติ

หมายเหตุ ข้อมูล ณ วันที่ 1 มิถุนายน 2563