ด่วนมาก บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๑๐๘๒)
ที่ กห ๐๖๐๙.๓/๔๒๗ **วันที่** ๕ ก.ค.๖๘
เรื่อง ขอให้ นขต.ทอ.และ นกข.ดำเนินการตามมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

เสนอ นขต.ทอ.

๑. ด้วยสถานการณ์ความขัดแย้งระหว่างประเทศในปัจจุบัน ตรวจพบความพยายามปฏิบัติการสงครามไซเบอร์ และปฏิบัติการข้อมูลข่าวสารจากฝ่ายตรงข้าม โดย ผบ.ทอ.สั่งการในที่ประชุม ทอ. ครั้งที่ ๖/๖๘ เมื่อ ๓๐ มิ.ย.๖๘ ให้ นขต.ทอ.และ นกข.ยกระดับมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อรับมือการโจมตีจากกลุ่มแฮกเกอร์และผู้ไม่หวังดีอย่างเร่งด่วน รวมทั้งเฝ้าระวังข้อมูลที่อาจส่งผลกระทบต่อความมั่นคง และให้มีการแลกเปลี่ยนข้อมูลภัยคุกคามจากหน่วยงานพันธมิตรอย่างต่อเนื่อง

๒. ทสส.ทอ.ตรวจสอบแล้ว ดังนี้

๒.๑ ผบ.ทอ.อนุมัติ เมื่อ ๒๓ มิ.ย.๖๓ ท้ายหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๔๒๖ ลง ๑๕ มิ.ย.๖๓ กำหนดให้เครื่องคอมพิวเตอร์สำนักงานที่ใช้ภายใน ทอ.ติดตั้งและใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และให้ นขต.ทอ.ตรวจสอบและกำกับดูแลการติดตั้งซอฟต์แวร์พื้นฐาน ให้เป็นไปตามแนวทางการติดตั้งใช้งานซอฟต์แวร์พื้นฐานสำหรับเครื่องคอมพิวเตอร์สำนักงานภายใน ทอ. และปรับปรุงเวอร์ชันให้เป็นปัจจุบัน (แนบ ๑)

๒.๒ หนังสือ ศชบ.ทอ.ด่วน ที่ กห ๐๖๕๐.๓/๕๖๘ ลง ๔ มิ.ย.๖๘ กำหนดข้อแนะนำสำหรับเหตุการณ์การแจ้งเตือนจากระบบเฝ้าระวังภัยคุกคามภาครัฐ (Gamble Guard) ตรวจพบการฝังสคริปต์เว็บพนันในเว็บไซต์ ทอ. ให้ ทสส.ทอ.พิจารณากำกับดูแลเว็บไซต์ และการใช้งานระบบเทคโนโลยีสารสนเทศให้ปลอดภัย (แนบ ๒)

๒.๓ หนังสือ ศชบ.ทอ.ด่วน ที่ กห ๐๖๕๐.๓/๖๐๘ ลง ๑๑ มิ.ย.๖๘ กำหนดแนวทางการแก้ไขปัญหาอุปกรณ์เครือข่าย Aruba ที่ไม่ปลอดภัยต่อการใช้งาน โดยอัปเกรดระบบปฏิบัติการของอุปกรณ์ Aruba รุ่น AP-3**, AP-4** และ AP-5** ให้เป็นเวอร์ชันล่าสุด งดใช้งาน Aruba รุ่น AP-1** และ AP-2** จนกว่าจะมีการจัดหาอุปกรณ์รุ่นใหม่ใช้งานทดแทน (แนบ ๓)

๓. ทสส.ทอ.พิจารณาแล้ว เพื่อป้องกันภัยคุกคามทางไซเบอร์ และป้องกันกำลังพล ทอ. ไม่ให้ตกเป็นเครื่องมือในการปฏิบัติการข่าวสารของฝ่ายตรงข้าม จึงขอให้หน่วยดำเนินการ ดังนี้

๓.๑ สอ.ทอ.ตรวจสอบทรัพยากรคอมพิวเตอร์ภายในศูนย์ข้อมูล ทอ.ที่ให้บริการแก่ นขต.ทอ.หากไม่สามารถพิสูจน์ทราบผู้รับผิดชอบหรือสถานภาพการใช้งานได้ ให้พิจารณายกเลิกการให้บริการและแจ้งให้ ทสส.ทอ.ทราบ

๓.๒ ศชบ.ทอ.ดำเนินการปิดกั้นคอมพิวเตอร์และอุปกรณ์เครือข่ายทั้งที่ใช้สายและไร้สายที่ตรวจพบว่ามีความสุ่มเสี่ยงต่อการละเมิดมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ จนกว่าจะได้รับการแก้ไข

๓.๓ นขต.ทอ. เน้นย้ำ กวดขัน กำกับดูแลกำลังพล ให้ระมัดระวังการส่งข้อมูลในช่องทางการสื่อสารต่าง ๆ ที่อาจส่งผลกระทบต่อความมั่นคง มีประเด็นความอ่อนไหวและปฏิบัติตามระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ อย่างเคร่งครัด

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ท.
จก.ทสส.ทอ.

- รอง ผอ.ศชบ.ทอ.และ ฝสธ.ศชบ.ทอ. ทราบ
- ทรอ. ดำเนินการ

พล.อ.ต.

ผอ.ศชบ.ทอ.

๒๕ /ก.ค./๖๕

- ทราบแล้ว
-

น.อ.

รอง ผอ.ศชบ.ทอ.

...../ก.ค./๖๕

- ทราบแล้ว
-

น.อ.

ฝสธ.ศชบ.ทอ.

...../ก.ค./๖๕

- ทราบแล้ว
-

น.อ.

รอง ผอ.ศชบ.ทอ.

...../ก.ค./๖๕

- ทราบแล้ว
-

น.อ.

ฝสธ.ศชบ.ทอ.

...../ก.ค./๖๕

ทราบแล้ว - ทราบทั่วกัน, ผพร.๑ ดำเนินการในส่วนที่เกี่ยวข้อง

น.อ.

หก.กฝพ.ศชบ.ทอ.

๒๖ /ก.ค./๖๕

ทราบแล้ว

น.ท.

รอง หก.กฝพ.ศชบ.ทอ.

๒๖ /ก.ค./๖๕

ทราบแล้ว

ร.ต.

นพร.ผพร.กฝพ.ศชบ.ทอ.

๒๖ /ก.ค./๖๕

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๑๐๘๒)

ที่ กห ๐๖๐๙.๓/๕๒๖ **วันที่** ๑๕ มิ.ย.๖๓

เรื่อง แนวทางการติดตั้งใช้งานซอฟต์แวร์พื้นฐานสำหรับเครื่องคอมพิวเตอร์สำนักงานภายใน ทอ.

เรียน ผบ.ทอ.

๑. ตามอนุมัติ ผบ.ทอ.เมื่อ ๘ มี.ค.๕๖ ท้ายหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๒๑๒ ลง ๒๘ ก.พ.๕๖ ให้ ทสส.ทอ.ตรวจสอบและรักษาการให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ ทอ. โดยนโยบายฯ หมวด ๗ กล่าวถึงการป้องกันชุดคำสั่งไม่พึงประสงค์ ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งใช้แฟ้มข้อมูล (File) อื่นที่ ทอ.ไม่อนุญาตให้ใช้งาน และหมวด ๑๔ กล่าวถึงการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์คอมพิวเตอร์ กำหนดให้โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยต้องเป็นโปรแกรมที่ ทอ.ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย นั้น (แนบ ๑)

๒. ทสส.ทอ.ตรวจสอบแล้ว ดังนี้

๒.๑ ซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์สำนักงานภายใน ทอ.ส่วนใหญ่เป็นซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ การติดตั้งใช้งานจะต้องทำการปลดล็อค (Crack) เพื่อให้เครื่องสามารถใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ได้เสมือนเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ซึ่งการปลดล็อค (Crack) จะมีการเปิดช่องโหว่หรือยกเลิกการรักษาความปลอดภัยของระบบ จึงอาจถูกโจมตีทางไซเบอร์ และข้อมูลต่าง ๆ ในเครื่องคอมพิวเตอร์อาจถูกขโมยหรือทำให้เกิดความเสียหาย

๒.๒ ซอฟต์แวร์ที่มีการติดตั้งและใช้งานใน ทอ.ในปัจจุบัน ยังไม่มีการกำหนดประเภทซอฟต์แวร์ที่อนุญาตให้ติดตั้งสำหรับเครื่องคอมพิวเตอร์สำนักงานที่ใช้ภายใน ทอ. จึงทำให้ไม่สามารถแลกเปลี่ยนข้อมูลและทำงานร่วมกันได้อย่างมีประสิทธิภาพ

๓. ทสส.ทอ.ได้ประชุมหารือกับ นกช.แล้ว เพื่อให้การติดตั้งและใช้งานซอฟต์แวร์ของ นขต.ทอ. เป็นไปในทิศทางเดียวกัน ถูกต้องตามกฎหมายไม่ละเมิดลิขสิทธิ์ และลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ จึงได้กำหนดแนวทางการดำเนินการ ดังนี้

๓.๑ กำหนดให้เครื่องคอมพิวเตอร์สำนักงานที่ใช้ภายใน ทอ.ติดตั้งและใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

๓.๒ กำหนดประเภทซอฟต์แวร์ที่อนุญาตให้ติดตั้งสำหรับเครื่องคอมพิวเตอร์สำนักงานที่ใช้ภายใน ทอ.ให้เป็นไปตาม คุณลักษณะซอฟต์แวร์พื้นฐาน ทอ.(แนบ ๒) โดยมีการกำหนดชนิดและรุ่นของซอฟต์แวร์ ๓ กลุ่ม ดังนี้

๓.๒.๑ ซอฟต์แวร์พื้นฐาน ประกอบด้วยโปรแกรมที่เป็นรุ่นและเวอร์ชัน ดังนี้

๓.๒.๑.๑ โปรแกรมระบบปฏิบัติการ ได้แก่

๓.๒.๑.๑ (๑) Microsoft Windows ให้ติดตั้งรุ่น Microsoft Windows 10 หรือใหม่กว่า

๓.๒.๑.๑ (๒) macOS ให้ติดตั้งรุ่น macOS Catalina หรือใหม่กว่า

๓.๒.๑.๑ (๓) Linux ให้ติดตั้งรุ่นและเวอร์ชันที่เป็นปัจจุบัน

๓.๒.๑.๒ โปรแกรม...

๓.๒.๑.๒ โปรแกรมสำนักงาน ได้แก่

๓.๒.๑.๒ (๑) Microsoft Office ให้ติดตั้งรุ่น Microsoft Office 2013 หรือใหม่กว่า

๓.๒.๑.๒ (๒) Libre Office ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๑.๓ โปรแกรมป้องกันไวรัส หรือโปรแกรมป้องกันมัลแวร์ ได้แก่

๓.๒.๑.๓ (๑) โปรแกรมตามที่ ศชบ.ทอ.แนะนำหรือสนับสนุน

๓.๒.๑.๓ (๒) โปรแกรมที่หน่วยจัดหาเอง ได้แก่ Kaspersky, Norton, McAfee, Bitdefender, Avira และ Trendmicro ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๑.๔ โปรแกรมเบราว์เซอร์ (Browser) กำหนดให้ใช้โปรแกรม Microsoft Edge, Internet Explorer, Google Chrome และ Mozilla Firefox ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๑.๕ โปรแกรมอ่านไฟล์ PDF กำหนดให้ใช้โปรแกรม Adobe Acrobat Reader, PDFescape และ PDF Reader ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๒ ซอฟต์แวร์เฉพาะทาง ประกอบด้วย

๓.๒.๒.๑ โปรแกรมดูและตัดต่อภาพ เป็นโปรแกรมสร้าง เปิด แก้ไข หรือปรับแต่งภาพนิ่ง เพื่อใช้ในการประชาสัมพันธ์ของหน่วย เช่น Microsoft Photo, ACDSee, Photo Scape, Adobe Photoshop หรือ Adobe Illustrator เป็นต้น

๓.๒.๒.๒ โปรแกรมเล่นและตัดต่อวิดีโอ เป็นโปรแกรมสร้าง เปิด แก้ไข หรือปรับแต่ง วิดีโอ หรือมัลติวิชันเพื่อใช้ในการประชาสัมพันธ์ของหน่วย เช่น Movie Media Player, Vegas, Adobe Premiere, Final Cut หรือ iMovie เป็นต้น

๓.๒.๒.๓ โปรแกรมบีบอัดข้อมูล เป็นโปรแกรมเพื่อใช้ในการบีบอัดย่อขนาดไฟล์ช่วยให้ทำให้ประหยัดเนื้อที่ในการจัดเก็บ และสามารถรวบรวมไฟล์เป็นแพ็คเกจ (Package) เดียวกันเพื่อสะดวกในการส่งต่อไปยังผู้ใช้อื่น ๆ เช่น WinZip, WinRAR หรือ Microsoft Compressed เป็นต้น

๓.๒.๒.๔ โปรแกรมเฉพาะทางสายวิทยาการ เช่น ArcGIS, Sketchup, AutoCAD, โปรแกรมเข้ารหัส-ถอดรหัส, ระบบสารสนเทศด้านการส่งกำลังบำรุง ทอ.(LMIS), ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) และระบบควบคุมการใช้จ่ายงบประมาณภายใน ทอ.(IBCS) เป็นต้น

๓.๒.๒.๕ โปรแกรมจัดการหรือแก้ไขไฟล์ PDF กำหนดให้ใช้โปรแกรม Adobe Acrobat Pro, PDFescape Editor หรือ Foxit Editor ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๒.๖ โปรแกรม หรือซอฟต์แวร์ที่ใช้สำหรับประชุมออนไลน์ กำหนดให้ใช้ Zoom Cloud Meeting, Cisco WebEx Meetings ที่เป็นเวอร์ชันและรุ่นปัจจุบัน

๓.๒.๓ ซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เอง โดย ศชว.ทอ.(เพื่อพลาง) หรือ นขต.ทอ. แบ่งออกเป็น ๒ กลุ่ม คือ กลุ่มงานด้านยุทธการ และกลุ่มงานด้านการสนับสนุน เป็นการพัฒนาเพื่อใช้ในการปฏิบัติงานใน ทอ. หรืออื่น ๆ

๔. ทสส.ทอ.พิจารณาแล้ว เพื่อให้การติดตั้งใช้งานซอฟต์แวร์พื้นฐานสำหรับเครื่องคอมพิวเตอร์สำนักงานภายใน ทอ. มีความปลอดภัยทางไซเบอร์และเป็นมาตรฐานเดียวกันทั้งระบบ เห็นสมควรดำเนินการ ดังนี้

๔.๑ นขต.ทอ.

๔.๑.๑ ตรวจสอบและกำกับดูแลการติดตั้งซอฟต์แวร์พื้นฐานให้เป็นไปตามข้อ ๓.๒.๑

๔.๑.๒ สำรวจ...

๔.๑.๒ สำรวจสถานภาพการติดตั้งใช้งานซอฟต์แวร์พื้นฐานของหน่วยตามที่กำหนดในข้อ ๓.๒.๑ และรายงานผลให้ ทสส.ทอ.ทราบ ตามแบบสำรวจซอฟต์แวร์พื้นฐาน นชต.ทอ. หรือ QR Code ที่ระบุ (แนบ ๓)

๔.๑.๓ การจัดทำโครงการจัดหาเครื่องคอมพิวเตอร์ทดแทนของหน่วย ให้กำหนดความต้องการซอฟต์แวร์พื้นฐานและซอฟต์แวร์เฉพาะทางที่มีลิขสิทธ์ถูกต้องตามกฎหมาย ตามที่กำหนดในข้อ ๓

๔.๑.๔ ปรับปรุงเวอร์ชัน (Update Patch) ของซอฟต์แวร์พื้นฐาน ที่ใช้ภายในหน่วยงานให้เป็นปัจจุบันอยู่เสมอ

๔.๑.๕ การติดตั้งซอฟต์แวร์เฉพาะทางที่นอกเหนือจากที่กำหนดในข้อ ๓.๒.๒ ให้หน่วยแจ้งความต้องการมาที่ ทสส.ทอ.เพื่อตรวจสอบความเหมาะสม

๔.๑.๖ การติดตั้งซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เองตามข้อ ๓.๒.๓ ให้หน่วยแจ้ง ทสส.ทอ.เพื่อตรวจสอบความเหมาะสม ก่อนนำมาติดตั้งใช้งาน

๔.๒ ทสส.ทอ.

๔.๒.๑ ควบคุม กำกับดูแลการปฏิบัติของ นชต.ทอ.ให้เป็นไปตามข้อ ๓

๔.๒.๒ ให้คำแนะนำการใช้งานซอฟต์แวร์เฉพาะทางที่นอกเหนือจากที่กำหนดในข้อ ๓.๒ ให้มีความเหมาะสมกับการปฏิบัติงานในสำนักงานให้กับ นชต.ทอ. หากตรวจสอบแล้วไม่มีความเหมาะสมให้แนะนำซอฟต์แวร์ที่มีคุณลักษณะใกล้เคียงเพื่อจัดทำโครงการฯ

๔.๒.๓ ประสานให้ ศชบ.ทอ.ตรวจสอบความปลอดภัยทางไซเบอร์ก่อนจัดหาซอฟต์แวร์เฉพาะทาง หรือซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เองของ นชต.ทอ.

๔.๒.๔ ประสานให้ ศชว.ทอ.(เพื่อพลาง) รับรองซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เองของ นชต.ทอ.

๔.๓ ศชบ.ทอ.

๔.๓.๑ ตรวจสอบความปลอดภัยทางไซเบอร์ของซอฟต์แวร์เฉพาะทางของหน่วยตามข้อ ๔.๑.๕ และ ๔.๑.๖ แล้วแจ้งผลการตรวจสอบให้ ทสส.ทอ.ทราบ

๔.๓.๒ ให้คำแนะนำการปรับปรุงเวอร์ชัน (Update Patch) ของซอฟต์แวร์พื้นฐานหรือติดตั้งโปรแกรมป้องกันมัลแวร์อื่น ๆ ที่มีความสามารถในการป้องกันทางไซเบอร์

๔.๔ ศชว.ทอ.(เพื่อพลาง)

๔.๔.๑ พัฒนาซอฟต์แวร์ตามข้อ ๓.๒.๓

๔.๔.๒ แจ้งผลการรับรองซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เองตามข้อ ๓.๒.๓ ให้ ทสส.ทอ.ทราบ

๔.๕ สอ.ทอ.

๔.๕.๑ กำหนดขอบเขตงาน (TOR) โครงการจัดหาเครื่องคอมพิวเตอร์ให้ครอบคลุมถึงซอฟต์แวร์พื้นฐานและซอฟต์แวร์เฉพาะทางที่มีลิขสิทธิ์ที่ถูกต้องตามกฎหมายทุกครั้ง

๔.๕.๒ ร่วมกับ ศชบ.ทอ.ตรวจสอบระบบเครือข่ายสารสนเทศและเครื่องคอมพิวเตอร์สำนักงาน ให้มีความปลอดภัย สามารถป้องกันการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ

๔.๕.๓ สนับสนุนเครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับติดตั้งซอฟต์แวร์ที่พัฒนาขึ้นมาใช้เองในข้อ ๓.๒.๓ หรือตามที่ นชต.ทอ.ร้องขอ

จึงเรียนมาเพื่อพิจารณาอนุมัติตามข้อ ๔

พล.อ.ท.

จก.ทสส.ทอ.

[illegible]

รอง ผอ.สนผ.(ธก.)

๑๙ มิ.ย. ๒๓

เรียน ผบ.ทส.

กระทรวงพิจารณาแล้ว เห็นสมควร อนุมัติตามข้อ ๔

พล.อ.อ.

เสธ.ทส.

๒๒ มิ.ย.๒๓

อนุมัติตามข้อ ๔

พล.อ.อ.

ผบ.ทส.

๒๓ มิ.ย.๒๓

ฯ.

ด่วน

บันทึกข้อความ

ส่วนราชการ ศชบ.ทอ.(กรช.โทร๒-๐๑๘๑)
ที่ กห ๐๒๕๐.๗/๕๕๕ วันที่ ๙ มิ.ย.๖๘
เรื่อง ข้อแนะนำสำหรับเหตุการณ์การแจ้งเตือนจากระบบเฝ้าระวังภัยคุกคามภาครัฐ (Gamble Guard) ตรวจพบการฝังสคริปส์เว็บพนันในเว็บไซต์ ทอ.

เสนอ สอ.ทอ., ทสส.ทอ. และ พอ.

๑. ด้วย ศชบ.ทอ.มีภารกิจในการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ในระบบสารสนเทศ ทอ. และได้รับแจ้งว่ามีการตรวจพบการฝังสคริปส์ในเว็บไซต์ ทอ.จากระบบเฝ้าระวังภัยคุกคามภาครัฐ (Gamble Guard) นั้น

๒. ศชบ.ทอ.ตรวจสอบและดำเนินการ ดังนี้

๒.๑ เมื่อ ๗ พ.ค.๖๘ ตรวจพบการฝังสคริปส์ในเว็บไซต์ รพ.ทอ.(สีกัน) ทอ.โดเมน ritafhospital.rtaf.mi.th โดยมี URL ที่ได้รับผลกระทบ เช่น https://ritafhospital.rtaf.mi.th/wp-content/web/index.php?uay=dg+casino.me และ https://ritafhospital.rtaf.mi.th/wp-content/web/index.php?u ay=joker เป็นต้น

๒.๑.๑ กรชบ.ศปก.ทอ.ได้เปิดเคส หมายเลข ๒๕๐๕๐๗๐๑ และได้ประสานทาง นทสส.รพ.ทอ.(สีกัน) ทอ.เพื่อเข้าตรวจสอบเว็บไซต์ดังกล่าวพบสาเหตุเกิดจากไม่ได้รับการอัปเดตให้เป็นปัจจุบัน จึงทำให้มีช่องโหว่ที่สามารถถูกฝังสคริปส์เว็บพนันในเครื่องแม่ข่ายได้

๒.๑.๒ นทสส.รพ.ทอ.(สีกัน) ทอ.ประสานเจ้าหน้าที่ สอ.ทอ.ให้ดำเนินการลบไฟล์มัลแวร์จากเครื่องแม่ข่ายและตรวจซ้ำ เจ้าหน้าที่ สอ.ทอ.ไม่พบไฟล์ต้องสงสัยอื่น ๆ เพิ่มเติม จึงได้ทำการปิดเคสดังกล่าว เมื่อ ๒๓ พ.ค.๖๘

๒.๒ เมื่อ ๒๔ พ.ค.๖๘ ตรวจพบการฝังสคริปส์ในเว็บไซต์ สอ.ทอ.ในโดเมน comm.rtaf.mi.th โดยมี URL ที่ได้รับผลกระทบคือ https://comm.rtaf.mi.th/?p=41755

ศชบ.ศปก.ทอ.ตรวจสอบเว็บไซต์ดังกล่าวเมื่อ ๒๔ พ.ค.๖๘ แล้วไม่พบการฝังสคริปส์ที่เป็นอันตราย จึงไม่ได้มีการปิดเคส

๓. เพื่อการดำเนินการตามข้อ ๒ เป็นไปด้วยความเรียบร้อย ศชบ.ทอ.เห็นควรให้ ทสส.ทอ. พิจารณากำกับการดูแลเว็บไซต์ และการใช้งานระบบเทคโนโลยีสารสนเทศให้ปลอดภัย โดยมีข้อเสนอแนะ ดังนี้

๓.๑ ควรใช้โปรแกรมและลิขสิทธิ์ทุกประเภท เช่น Windows, Microsoft Office เป็นต้น

๓.๒ ใช้โปรแกรมฟรี (Freeware) ทดแทน Microsoft Office เช่น LibreOffice เป็นต้น

๓.๓ ใช้บริการ Odoo ในการพัฒนาเว็บไซต์ เพื่อให้มีความปลอดภัยมากขึ้น

๓.๔ มอบหมายให้มีผู้ดูแลระบบเว็บไซต์เฝ้าระวังอย่างต่อเนื่อง

๓.๕ ประสาน ศชบ.ทอ.ขอรับการสนับสนุนโปรแกรมตรวจจับภัยคุกคามที่เครื่องแม่ข่ายและเครื่องลูกข่าย (EDR) เช่น Trellix หรือ Bitdefender เป็นต้น

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.อ. ประภาส
ผอ.ศชบ.ทอ.

ด่วน

บันทึกข้อความ

ทสส.ทอ.
รับที่ ๒๒๔๙
วันที่ ๑๖ มิ.ย. ๒๕๖๘
เวลา ๑๔๓๖

ส่วนราชการ ศชบ.ทอ.(กรมโทร ๒-๐๑๘๑)
ที่ กท ๐๖๕๐.๗/๖๐๙ วันที่ ๑๒ มิ.ย.๖๘
เรื่อง แนวทางการแก้ไขปัญหาอุปกรณ์เครือข่าย Aruba ที่ไม่ปลอดภัยต่อการใช้งาน

เสนอ สอ.ทอ. และ ทสส.ทอ.

๑. ตามที่ ศชบ.ศปก.ทอ.ตรวจพบความไม่ปลอดภัยต่อการใช้งานอุปกรณ์เครือข่าย Aruba เมื่อ ๓๑ มิ.ย.๖๘ แสดงให้เห็นผู้ไม่หวังดีได้เจาะระบบของอุปกรณ์เครือข่าย Aruba ของ ทอ.จำนวนมาก แล้วทำการฝังโทรจันที่มีขีดความสามารถสั่งการจากระยะไกล เพื่อใช้อุปกรณ์ Aruba ในการแสกนและโจมตีเป้าหมายที่ผู้ไม่หวังดีต้องการต่อไป ซึ่งสร้างความไม่ปลอดภัยต่อการใช้งานเครือข่าย ทอ. และชื่อเสียงของ ทอ. รายละเอียดตามแนบ นั้น

๒. ศชบ.ทอ.ตรวจสอบและดำเนินการ ดังนี้

๒.๑ ประสาน สอ.ทอ.ได้รับข้อมูลว่ามีการใช้งานอุปกรณ์เครือข่าย Aruba ตั้งแต่รุ่น AP-1** จนถึง AP-5** กระจายการติดตั้งที่ นขต.ทอ.เพื่อให้บริการ RTAF-WiFi ให้กับกำลังพล ทอ.

๒.๒ เว็บไซต์ผู้ผลิตของ Aruba (hpe.com) ได้ประกาศแจ้งเตือน เมื่อ ๕ พ.ย.๖๗ ตรวจพบอุปกรณ์ Aruba มีช่องโหว่ระดับรุนแรง ประกอบด้วย CVE-2024-42509, CVE-2024-47460, CVE-2024-47461, CVE-2024-47462, CVE-2024-47463 และ CVE-2024-47464 ซึ่งทำให้ผู้ไม่ประสงค์ดีใช้เจาะระบบและยึดอุปกรณ์ได้ อุปกรณ์ Aruba ที่ได้รับผลกระทบประกอบด้วยรุ่น AP-1**, AP-2**, AP-3**, AP-5** และ AP-6**

๒.๓ การแก้ไขช่องโหว่ข้างต้นสามารถทำได้ โดยอัปเกรดระบบปฏิบัติการของอุปกรณ์ Aruba ให้เป็นเวอร์ชันล่าสุด

๒.๔ พบอุปสรรคในการแก้ไขช่องโหว่เนื่องจาก Aruba รุ่น AP-1** และ AP-2** พ้นระยะเวลาการสนับสนุนจากผู้ผลิต จึงไม่มีระบบปฏิบัติการเวอร์ชันใหม่ที่ใช้อัปเกรดเพื่ออุดช่องโหว่ได้

๒.๕ แนวทางแก้ไขปัญหา ดังนี้

๒.๕.๑ อัปเกรดระบบปฏิบัติการของ Aruba รุ่น AP-3**, AP-4** และ AP-5** ให้เป็นเวอร์ชันล่าสุด

๒.๕.๒ งดใช้งาน Aruba รุ่น AP-1** และ AP-2** และจัดหาอุปกรณ์รุ่นใหม่ใช้งานทดแทน

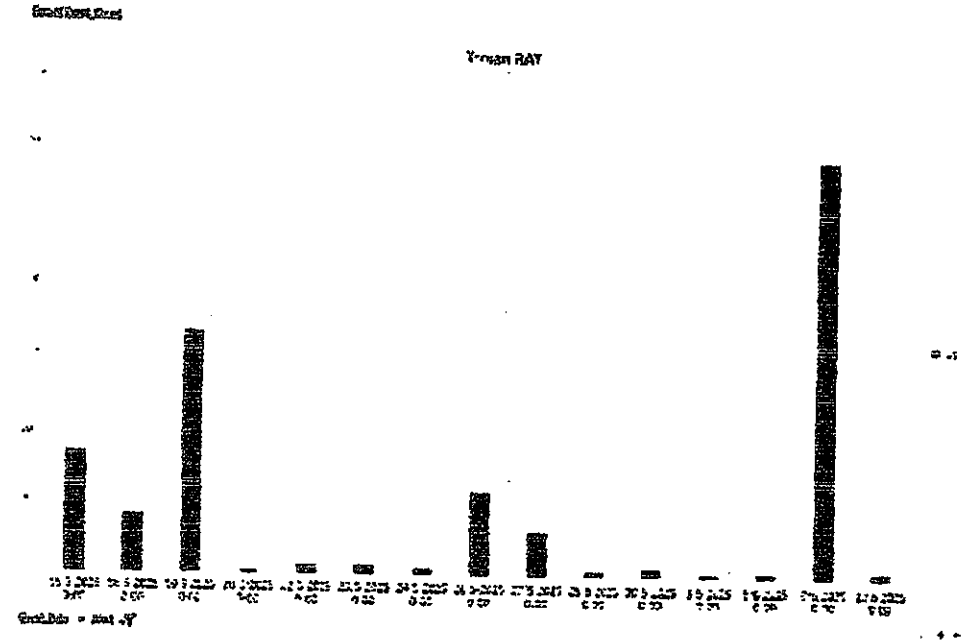
๒.๕.๓ วางแผนจัดหาอุปกรณ์ทดแทน Aruba AP-3** ที่จะพ้นระยะเวลาสนับสนุนจากผู้ผลิตในปี ๖๙

๓. ศชบ.ทอ.พิจารณาแล้ว เพื่อแก้ไขปัญหาอุปกรณ์เครือข่าย Aruba ที่ไม่ปลอดภัยต่อการใช้งาน จึงขอให้ผู้เกี่ยวข้องดำเนินการตามแนวทางแก้ไขปัญหา ตามข้อ ๒.๕ ทั้งนี้มอบหมายให้ น.อ.เอกชัย สิงห์ทอง รอง ผอ.กรม.ศชบ.ทอ.โทร ๒-๐๑๘๑ หรือ โทร ๐๖ ๔๒๗๕ ๕๕๕๓ เป็นผู้ติดต่อประสานโดยตรง

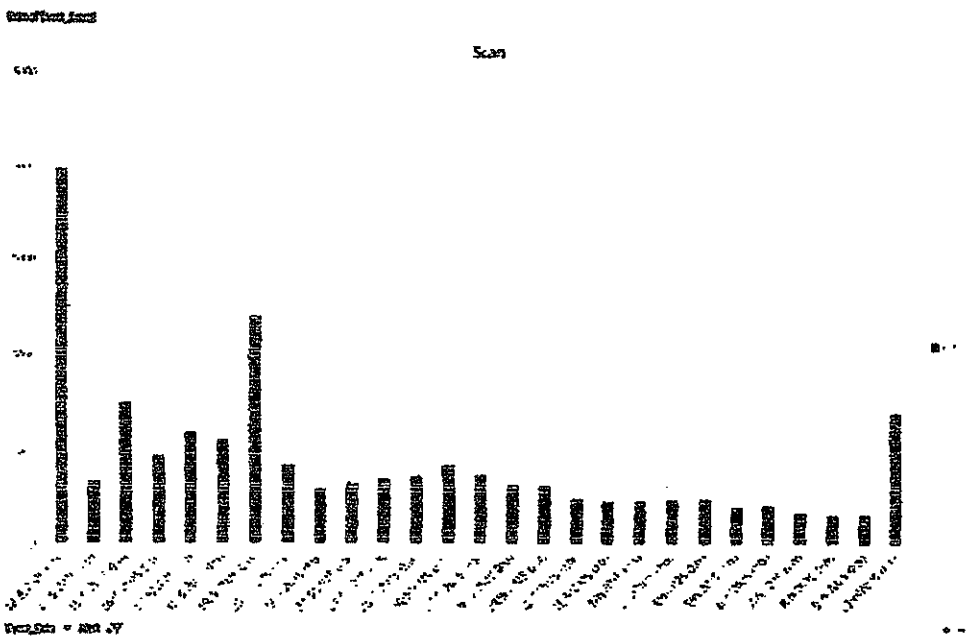
จึงเสนอมาเพื่อดำเนินการให้ต่อไป

พล.อ.ต. [ลายเซ็น]
ผอ.ศชบ.ทอ.

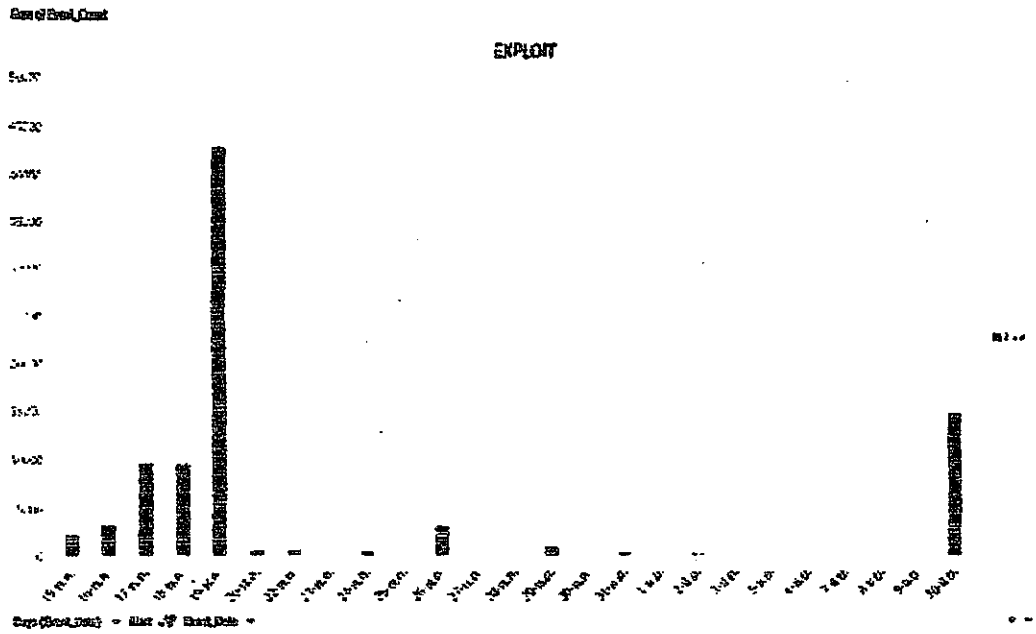
รายงานการตรวจพบความไม่ปลอดภัยต่อการใช้งานอุปกรณ์เครือข่าย Aruba



ภาพที่ ๑ สถิติอุปกรณ์เครือข่าย Aruba มีการเชื่อมต่อไปยังเครื่องบัญชาการและควบคุมของ โทรจัน ที่สามารถควบคุมสั่งการจากระยะไกลได้ (Trojan RAT) ห้วง ๑๕ พ.ค. - ๑๐ มิ.ย.๖๘



ภาพที่ ๒ สถิติอุปกรณ์เครือข่าย Aruba ทำการสแกนออกไปนอกเครือข่าย ทอ. ห้วง ๑๖ พ.ค. - ๑๐ มิ.ย.๖๘ ซึ่งบอกถึงอุปกรณ์เครือข่าย Aruba ถูกใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์



ภาพที่ ๓ สถิติอุปกรณ์เครือข่าย Aruba ทำการโจมตีเจาะระบบไปยังเป้าหมายนอกเครือข่าย ทอ. ห้วง ๑๕ พ.ค. - ๑๐ มิ.ย.๖๘ ซึ่งนอกเหนือจากอุปกรณ์เครือข่าย Aruba ถูกใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์

ขอรับรองว่าถูกต้อง
น.อ.
(เอกชัย สิงห์ทอง)
รอง ผอ.กรม.ศชบ.ทอ./
หน.ชุดเผชิญเหตุทางไซเบอร์ ศชบ.ศปก.ทอ.
๑๖ มิ.ย.๖๘