# Cyber Warfare ตอนที่1: 8 ขั้นตอนปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์

ในปัจจุบันคอมพิวเตอร์และเทคโนโลยีสารสนเทศได้มีการพัฒนาอย่างต่อเนื่อง รวมถึงมีบทบาทในการทำงานแทบทุกแขนงในภาครัฐและเอกชน ซึ่งเป็นเทรนด์ของโลกยุคสมัยใหม่ (4.0 Age) ตามนิยามของโลกโลกาภิวัตน์ที่มีการแข่งขันทางเทคโนโลยีอย่างรุนแรง ซึ่งเป็นหนึ่งในปัจจัยที่ผู้ครอบครองเทคโนโลยีสารสนเทศขั้นสูงจะสามารถใช้ประโยชน์จากข้อมูลและความรู้ที่มีสร้างนวัติกรรมต่าง ๆ ให้เกิดขึ้นได้ในทุกองคาพยพตั้งแต่ระดับการใช้งานในชีวิตประจำวัน จนกระทั่งองค์ความรู้ที่มีความซับซ้อนสูง เช่น เทคโนโลยีอวกาศ หรือการทหารอีกด้วย

นอกจากนี้ในกองทัพของทุกประเทศ ระบบอาวุธยุทโธปกรณ์ก็มีความก้าวหน้าขึ้อย่างรวดเร็ว พร้อม ๆ กับการพัฒนาทางยุทธวิธีที่เปลี่ยนแปลงจากการใช้กำลังรบแต่ละหน่วยโดยอิสระ (Independent unit) ที่เน้นอำนาจการยิงในการเข้าปะทะ (Firepower) ไปสู่การรบแบบเป็นกลุ่มก้อนประสานงานโดยใกล้ชิดผ่านเครือข่าย (Network Based) พร้อมทั้งอาวุธประสิทธิภาพสูง (Smart Weapon) เพื่อเพิ่มบูรณาการศักยภาพของระบบอาวุธร่วมกันได้สูงสุด (Utilization) ซึ่งการดำเนินการดังกล่าวจำเป็นต้องมีการบริหารจัดการระบบบัญชาการและควบคุม (Command Control) อย่างใกล้ชิดและรวดเร็วที่สุด จึงจำเป็นต้องสร้างเครือข่ายเข้าหากันเพื่อให้เกิดการเชื่อมต่อแบบอัตโนมัติ แทนการรายงานด้วยอาณัติสัญญาณแบบต่าง ๆ ของกำลังพล (Manual Signal) ซึ่งการพัฒนาระบบดังกล่าวล้วนแต่จำเป็นต้องกระทำผ่านเครือข่ายคอมพิวเตอร์ทั้งสิ้น ชนิดที่เรียกได้ว่าในยุคปัจจุบัน (ค.ศ.2000 ขึ้นไป) ได้กลายเป็นยุคการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางทุก ๆ ด้าน ตั้งแต่ สายการบังคับบัญชาการควบคุม ข้อมูลทางยุทธวิธี การส่งกำลังบำรุง การวางกำลังยุทโธปกรณ์ การจัดสรรแนวป้องกันและส่วนสนับสนุน เป็นต้น

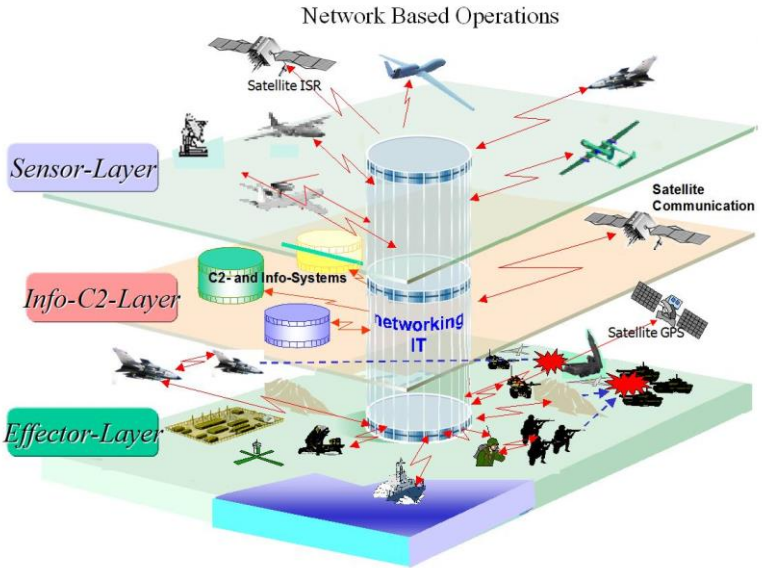


*Figure1 : Network Base Operation*[1]

อย่างไรก็ตาม ระบบสารสนเทศของกองทัพเองก็มีความเป็นไปได้ที่จะเป็นเป้าหมายของการถูกโจมตี (Vulnerability) ได้เช่นเดียวกับเป้าหมายที่มีความสำคัญสูง (High Value Target) อื่น ๆ ของกองทัพ เนื่องจาก หากเครือข่ายคอมพิวเตอร์ดังกล่าวถูกรบกวน ขัดขวาง โจมตี เปลี่ยนแปลง จนไม่อาจทำงานได้ตามปกติ จะทำให้กองทัพสูญเสียความสามารถในการตอบสนองต่อภัยคุกคามลงอย่างมาก ซึ่งปฏิบัติการจู่โจมเหล่านี้ ได้สร้างรูปแบบการสงครามชนิดใหม่ขึ้นมาที่เรียกว่า “สงครามไซเบอร์” (Cyber Warfare) ซึ่งเป็นกระบวนการโจมตีที่มุ่งให้เกิดผลกระทบต่อระบบเครือข่ายของฝ่ายตรงข้ามอันเรียกว่า Cyber Space

นิยามฯ ของระบบเครือข่ายฯ นั้นมีหลากหลายตามแต่ละผู้วิจัยพัฒนาได้กำหนดไว้ ในบทความนี้ขอยกตัวอย่าง เช่น นิยามของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.:ETDA) ได้กล่าวถึง Cyber Space ไว้ว่า *“ระบบ บริการ การสื่อสาร ที่เชื่อมต่อทั้งทางตรงหรือทางอ้อมเข้ากับอินเตอร์เน็ต โทรคมนาคม และเครือข่ายคอมพิวเตอร์ พร้อมทั้งข้อมูลและสารสนเทศในระบบบริการนั้น”* ซึ่งใกล้เคียงกับการใช้งานทางการทหารที่มีการเชื่อมโยงหลายรูปแบบ ทั้งจากอุปกรณ์ทางยุทธวิธีและบุคลากรทางอ้อม สามารถใช้เพื่อการรวบรวมข้อมูล โจมตี หรือปกป้องระบบของตน คล้ายคลึงกับกระบวนการของสงครามอิเล็กทรอนิคส์ (EW: Electronic Warfare) ที่มีการใช้งาน ECM (การตอบโต้ทางอิเล็กทรอนิคส์) ECCM (การตอบโต้ - การตอบโต้ทางอิเล็กทรอนิคส์) และ ESM(การสนับสนุนทางอิเล็กทรอนิคส์) ได้เช่นกัน โดยในทางการทหารปฏิบัติการสงครามไซเบอร์นั้น มักมุ่งเป้าไปสู่การปฏิบัติการเครือข่ายคอมพิวเตอร์ (CNO: Computer Network Operation) ซึ่งถือเป็นประเด็นหลัก อันประกอบไปด้วยปฏิบัติการ 3 ประเภท

- ปฏิบัติการใช้ประโยชน์เครือข่ายคอมพิวเตอร์ (CNE: Computer Network Exploitation)
- ปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ (CNA: Computer Network Attack)
- ปฏิบัติการป้องกันเครือข่ายคอมพิวเตอร์ (CMD: Computer Network Defense)

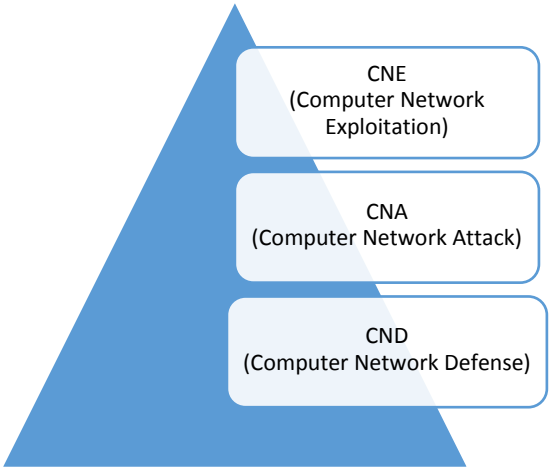


*Figure 2: การปฏิบัติการเครือข่ายคอมพิวเตอร์ (CNO)*

การจู่โจมเครือข่ายคอมพิวเตอร์นั้น มีกระบวนการ แผนงาน และยุทธวิธีที่ต้องปฏิบัติ (Protocol) พร้อมทั้งใช้งานยุทโธปกรณ์เข้าโจมตีเป้าหมาย เช่นเดียวกับการที่กองทัพจะใช้กำลังรบเข้าตีที่มั่นของข้าศึก แต่มีจุดที่แตกต่างกันอย่างเด่นชัด 2 ข้อ คือ

- พื้นที่ยุทธบริเวณนั้นยากต่อการระบุถึงทางกายภาพ เช่น ที่หมายข้าศึกไม่ใช่ค่าพิกัดบนแผนที่ภูมิศาสตร์อีกต่อไป แต่เป็นชื่อของเว็ปไซต์ (Domain Name) หมายเลขระบุตัวตน (IP-Address) ซึ่งไม่อาจระบุแน่ชัดว่าจัดเก็บระบบงานอยู่ส่วนใดบนโลกได้อย่างชัดเจน
- ยุทโธปกรณ์ที่ใช้ ทั้ง Software, Hardware และวงจรสื่อสารต่างๆ ไม่สร้างความเสียหายให้กับชีวิตของบุคลากรทั้งฝ่ายโจมตีและฝ่ายถูกโจมตี (Zero Casualty)

สอดคล้องกับหลักนิยมการรบสมัยใหม่ที่มุ่งเน้นไปถึงเรื่องการลดการถูกตรวจจับ (low observable) อาทิ ระบบล่องหน (Stealth) ระบบอาวุธไร้คนขับ (Unman Vehicle) สงครามทางไซเบอร์ที่มุ่งเน้นจู่โจมเสมือน (Virtual Attack) จัดเป็นตัวอย่างที่ดีมากในการใช้งานจริง และด้วยความที่พิสูจน์ตัวตนที่มาของผู้จู่โจมได้ยาก อีกทั้งง่ายต่อการที่รัฐต่าง ๆ จะปฏิเสธความรับผิดชอบต่อคู่กรณี แม้จะมีการใช้งานจริง โดยการปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ (CNA) นั้นหมายถึง การก่อกวน ปฏิเสธ ลดประสิทธิภาพ หรือทำลายตัวข้อมูลที่อยู่ในระบบเครือข่ายคอมพิวเตอร์ (Attack Data) หรือตัวเครื่องในระบบเครือข่ายคอมพิวเตอร์นั้นเอง (Attack Hardware) โดยระบบดังกล่าวหมายถึง ระบบงานที่ใช้ในการสงคราม เช่น การบัญชาการและควบคุม (Command and Control) เครือข่ายป้องกันภัยทางอากาศ เป็นต้น

ซึ่งในบทความ Cyber Warfare ตอนที่ 1 นี้จะมุ่งเน้นไปยังกระบวนการโจมตีเครือข่ายคอมพิวเตอร์ (CNA) ทั้ง 8 รูปแบบ เพื่อเห็นถึงแนวทางการจู่โจมระบบงานสารสนเทศที่เป็นไปได้ ดังนี้

1. การลาดตระเวณ (Recon)
2. การสแกน (Scan)
3. การเข้าถึง (Access)
4. การเพิ่มสิทธิ์ (Escalate)
5. การดึงข้อมูล (Extrude)
6. การโจมตี (Assault)
7. การคงอยู่ (Sustain)
8. การซ่อนพราง (Obfuscate)

1. **<u>การลาดตระเวณ (Recon)</u>**

ขั้นตอนแรกของกระบวนการโจมตีเป้าหมายทางไซเบอร์ คือการรวบรวมข้อมูลพื้นฐานของเป้าหมาย (Target) จากแหล่งข้อมูลทั้งส่วนที่เป็นสาธารณะ (Public Data) และข้อมูลภายใน (Private Data) ที่มีการเปิดเผยหรือสืบทราบได้จากแหล่งข่าวอื่น ๆ ที่มี อาทิเช่น

- ข้อมูลพื้นฐานของระบบเป้าหมาย ได้แก่ ชื่อเว็ปไซต์ (Domain Name) นามสกุล เวปที่จดทะเบียนอยู่ (Provider) ซึ่งจะช่วยให้ทราบว่าเป้าหมายมีสังกัดหรือใช้บริการจากที่ใดบ้างเพื่อตรวจสอบสภาพแวดล้อม (ECO System) โดยรวม
- ข้อมูลภายใน เช่น สถานที่จัดวางเครื่องแม่ข่าย (Physical Server) ช่องทางติดต่อผู้ดูแลระบบ (Admin Contact) เพื่อให้ทราบถึงแหล่งข้อมูลที่เป็นไปได้จะจู่โจมหรือการเข้าถึงเป้าหมายผ่านผู้ควบคุมระดับที่สูงขึ้นไป

กระบวนการลาดตระเวณนั้นมักเป็นส่วนนึงของการรวบรวมข้อมูลมุมกว้าง (Broad View) ของผู้โจมตี ซึ่งจะเป็นประโยชน์ต่อการคัดเลือกเหยื่อที่มีความเป็นไปได้ ในแง่ของความคุ้มค่าของข้อมูลที่ได้รับ หรือความซับซ้อนในการโจมตีที่ผู้ลงมือต้องทุ่มเทให้ในการจู่โจม อย่างเช่น การโจมตีระบบงานของโรงพยาบาล ธนาคาร หรือบริษัทที่มีความอ่อนไหวด้านชื่อเสียงสูง จะมีแนวโน้มที่ยอมจำนนต่อการโจมตีได้ง่ายเป็นพิเศษเมื่อเทียบกับบุคคลทั่วไป

*<u>แนวทางการป้องกัน</u>*

เนื่องจากระบบงานในไซเบอร์สเปซนั้น ส่วนมากสร้างขึ้นเพื่อให้ใช้ได้เป็นวงกว้างทั่วถึงอันเป็นการอำนวยความสะดวกให้กับผู้ปฏิบัติงานและองค์กร ซึ่งการป้องกันการลาดตระเวณโดยสมบูรณ์แบบนั้นมีวิธีการเดียว คือ การทำระบบงานทั้งหมดให้เป็นระบบปิด (Close System) ซึ่งทำให้การปฏิบัติงานของระบบขาดความคล่องตัวอย่างยิ่ง แนวทางการป้องกันที่เป็นที่นิยมในปัจจุบัน คือ แยกระบบงานส่วนที่สำคัญออกจากกัน (Separate Critical-Module) เพื่อหลีกเลี่ยงการสูญเสียข้อมูลสภาพแวดล้อมที่สำคัญออกไปพร้อมกัน

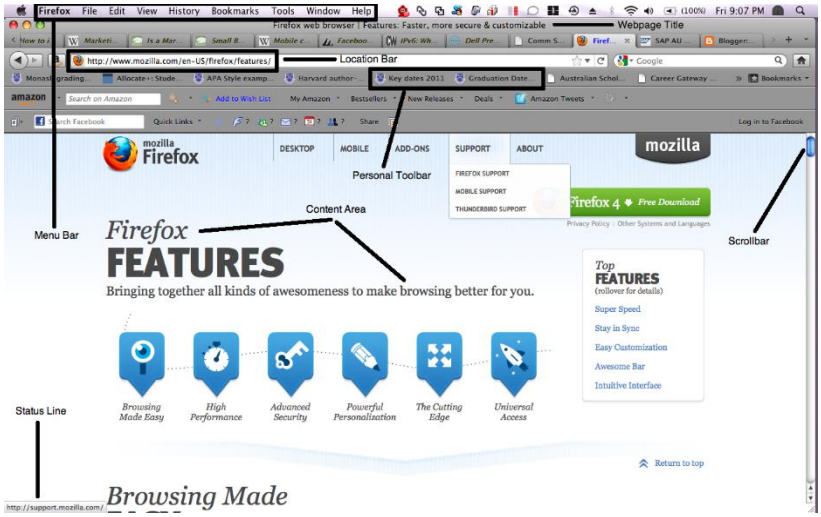


*Figure 3: การวิเคราะห์ส่วนประกอบของเว็ปไซต์เป้าหมาย*[3]

2. **<u>การสแกน (Scan)</u>**

เป็นขั้นตอนต่อเนื่องของการรวบรวมข้อมูลเบื้องต้นของเป้าหมายที่ผู้โจมตีคัดเลือกไว้ เพื่อจะประเมินช่องโหว่ จุดอ่อน จุดแข็งของระบบงาน เพื่อใช้เป็นข้อมูลก่อนตัดสินใจทำอย่างอื่นต่อไป รวมถึงการคัดเลือกเครื่องมือและวิธีการที่จะใช้โจมตี โดยเริ่มจากการสแกนจากอินเตอร์เน็ต โดยไม่มีข้อมูลล่วงหน้าใด ๆ เลย จนถึงการสแกนจากเครือข่ายภายใน และการแสกนผ่านเครือข่ายที่ระบบเป้าหมายให้ความเชื่อถือมาก่อน ซึ่งการสแกนหลายทิศทางนี้จะช่วยให้ทราบช่องโหว่แต่ละจุดที่จำเป็นว่าเมื่อเกิดการโจมตีขึ้นจริง ๆ จะมีโอกาสสำเร็จหรือไม่ โดยเรียกว่าการทำ “ฟุตพรินติง” (Footprinting)

ทั้งนี้ รูปแบบการสแกนที่ได้รับความนิยมมากที่สุด คือ การปิง (Ping) ซึ่งเป็นการส่งคำสั่งสัญญาณแบบนึงจากเครื่องของตนเอง (Host Machine) ไปยังเครื่องเป้าหมาย (Target-Machine) ซึ่งจะส่งสัญญาณกลับ (Echo) ไปให้ผู้ส่งคำสั่งมา สามารถใช้ตรวจสอบว่าเครื่องเป้าหมายเปิดทำงาน (Switch On) อยู่หรือไม่ ซึ่งหากหมายเลขที่อยู่ (Address) ใดไม่ส่งสัญญาณกลับก็จะข้ามไปยังหมายเลขถัดไปทันที ทำให้ผู้โจมตีสามารถประหยัดเวลาในการค้นหาเครื่องที่มีความเป็นไปได้ในการจู่โจมลงอย่างมาก

เมื่อผู้จู่โจมได้ทำการสแกนเบื้องต้นและคัดเลือกเป้าหมายที่ค้นพบ (Visible Target) แล้ว ก็สามารถเริ่มการสแกนขั้นสูงได้ต่อไป โดยใช้ชุดคำสั่งอื่น ๆ ร่วมกับการ Ping เพื่อค้นหาข้อมูลเชิงลึกมากขึ้นเรื่อย ๆ อันได้แก่ ช่องทางเชื่อมต่อระหว่างที่อยู่ (Address Port) การกระโดดเชื่อมต่อระหว่างที่อยู่ภายในของเหยื่อ (Net route) เพื่อให้เห็นภาพรวมของระบบงานได้มากที่สุดต่อไป

*<u>แนวทางการป้องกัน</u>*

การสแกนเป็นกระบวนการที่ผู้โจมตีเริ่มใช้คำสั่งต่าง ๆ ส่งเข้ามายังระบบงานของเป้าหมาย (Activity Run) ซึ่งจุดอ่อนสำคัญหลักของการสแกน คือ “เวลาที่ใช้” ที่ต้องค้นหาไปทีละระบบและเส้นทางภายใน

ซึ่งระบบงานทั่วไปที่ทำงานอยู่แล้วจะถูกตั้งค่าต่าง ๆ ไว้ล่วงหน้าจึงไม่จำเป็นต้องมีกระบวนการนี้ เจ้าของระบบที่เป็นฝ่ายตั้งรับสามารถใช้อุปกรณ์ (Hardware/Software) เพื่อป้องกันเครือข่ายภายในของตนเองได้ เช่น ไฟล์วอลร์ (Firewall) หรือ IDS (Intrusion Detection System) ซึ่งคอยสอดส่องพฤติกรรมที่ผิดปกติของการส่งข้อมูล และบีบบังคับให้ผู้ใช้คำสั่งสแกนจากภายนอก ต้องปฏิบัติตามเงื่อนไขเส้นทางอันเข้มงวดของอุปกรณ์เหล่านี้

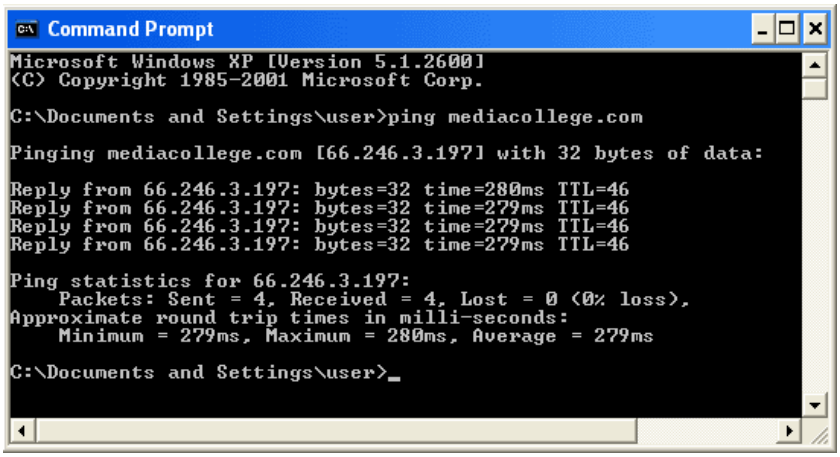


*Figure 4: การใช้คำสั่ง Ping แบบปกติ*

3. **<u>การเข้าถึง (Access)</u>**

เมื่อค้นหาช่องโหว่ของเป้าหมายพบแล้ว กระบวนการถัดมาคือการเลือกใช้เครื่องมือ (หรือโปรแกรม) ในการโจมตีผ่านช่องโหว่ดังกล่าว ซึ่งเครื่องมือเหล่านี้ สามารถค้นหาได้ทั่วไปทางอินเตอร์เน็ต หรือผู้มีทักษะเชี่ยวชาญอาจสร้างขึ้นมาเพื่อใช้เอง (Man-made) ก็ได้ ซึ่งเครื่องมือเหล่านี้เป็นสิ่งที่ใช้กันทั่วไปด้วยในงานด้านการศึกษาประเมินความปลอดภัยของโครงข่ายที่ตนเองใช้งานอยู่ จึงเปรียบได้กับเป็นดาบสองคม ตามแต่จุดประสงค์ของผู้ใช้งาน อาทิเช่น โปรแกรมเนสซัส (Nessus) ที่มีเครื่องมือในการโจมตีช่องโหว่ต่าง ๆ ของเป้าหมายผ่านโปรแกรมเสริมของระบบงานที่มีใช้อยู่ ซึ่งจะเรียกว่า ปลั๊กอิน (Plugin)

โดยปกติระบบปฏิบัติการ (OS: Operating System) และโปรแกรมประยุกต์ (Application) จะมีปลั๊กอินต่าง ๆ อยู่เป็นจำนวนมหาศาล เพื่อตอบสนองต่อความต้องการของผู้ใช้งานและผู้ดูแลระบบด้านต่าง ๆ อยู่แล้ว แต่โปรแกรมโจมตีระบบงาน เช่น เนสซัสนั้นจะบุกเข้าไปในระบบเป้าหมายเพื่อรวบรวมข้อมูลสภาพแวดล้อมก่อนแล้วคัดกรอง (Filter) เฉพาะปลั๊กอินที่เป็นไปได้ในการโจมตีในแต่ละสภาพแวดล้อมให้ ซึ่งประหยัดเวลาในการลองผิดลองถูกได้อย่างมาก

*แนวทางการป้องกัน*

การเข้าถึงระบบงานต่าง ๆ ของ Software จากภายนอกนั้นจะเกิดขึ้นภายใต้สภาพแวดล้อมของระบบงานดังกล่าวเสมอ ดังนั้น ผู้ดูแลระบบสามารถตั้งค่าระบบป้องกันภัยของตน เช่น Firewall ให้คอยสอดส่องดูแลระบบงานอย่างต่อเนื่องได้ แต่ทั้งนี้ จำเป็นต้องคอยตรวจสอบบันทึกสถานการณ์ (Log) ที่ระบบป้องกันภัยคอยรายงานอย่างสม่ำเสมอ เพื่อให้เห็นถึงสภาพผิดปกติของระบบภายใน รวมทั้งหมั่นปรับปรุง (Update) ตัวโปรแกรมปลั๊กอินอย่างรวดเร็วทุกครั้งที่มีการประกาศจากเจ้าของโปรแกรมเพื่อปิดช่องโหว่ที่โปรแกรมโจมตีจะสามารถเข้าถึงได้โดยไม่ได้รับอนุญาต

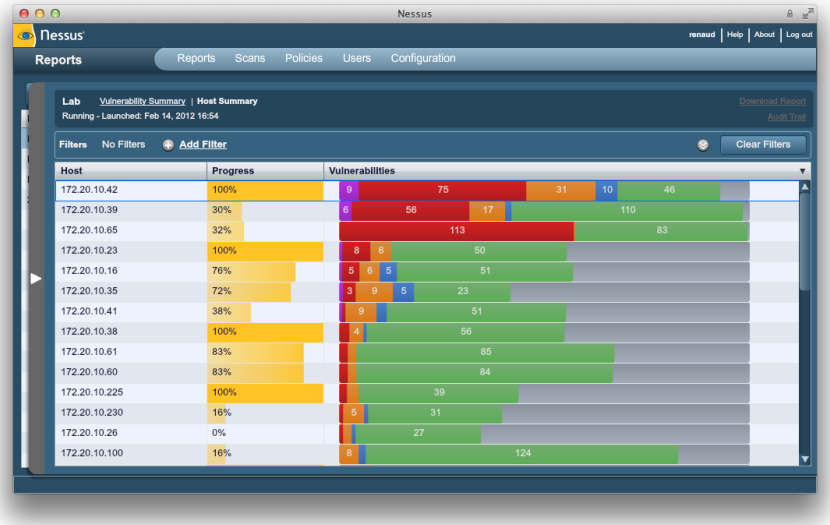


*Figure 5: ตัวอย่าง Software Nessus*

4. **การเพิ่มสิทธิ์ (Escalate)**

ในกรณีที่ผู้จู่โจมสามารถเจาะ/เข้าถึง (Access) ระบบงานเป้าหมายได้แล้ว โดยปกตินั้นการเข้ามาอาจเป็นแค่บัญชีผู้ใช้ทั่วไป (User Account) ซึ่งไม่มีสิทธิใด ๆ นอกจากการเข้าถึงข้อมูลบางส่วน ดังนั้น การที่จะทำการโจมตีหรือช่วงชิงข้อมูลสำคัญต่าง ๆ จำเป็นต้องหาวิธีเพิ่มสิทธิให้กับตนเอง (Privilege Escalation) เพื่อจะได้ทำการขยายผลการโจมตีในเครือข่ายนั้น ๆ ให้ได้ โดยมีการทำได้หลายวิธี ทั้งจากการใช้ประโยชน์จากช่องโหว่ของปลั๊กอิน ช่องโหว่ของการตั้งค่า (Configuration) ที่ไม่รัดกุม หรือการช่วงชิงสิทธิผู้ดูแลระบบ (Administrator/Root Account)

ทั้งนี้ วิธีที่ได้รับความนิยมมากที่สุด คือ การอาศัยช่องโหว่ของการตั้งค่าไม่รัดกุม (Configuration) ของโปรแกรมที่ผู้ใช้งานติดตั้งอยู่ในเครื่อง เปิดโอกาศให้ผู้จู่โจมได้สิทธิในการติดตั้งโปรแกรมประยุกต์บางอย่างเพิ่มเติมลงไปในเครื่องของเป้าหมาย ซึ่งสามารถยกระดับสิทธิให้เป็นผู้ดูแลระบบคนที่ 2 (Second Admin) ได้ในภายหลัง ซึ่งเมื่อได้สิทธิดังกล่าวแล้วทำให้ผู้โจมตีสามารถรับ – ส่งข้อมูลต่าง ๆ ได้อิสระเหมือนกับเป็น

บุคคลภายในโดยสมบูรณ์ ซึ่งจัดเป็นขั้นตอนที่อันตรายมากที่สุดสำหรับผู้ถูกจู่โจมเนื่องจากถูกบุกรุกถึงภายในสุดของระบบงานโดยที่ยังไม่รู้ตัว

<u>แนวทางการป้องกัน</u>

การเพิ่มสิทธิ์ (Escalation) จำเป็นอย่างยิ่งต้องได้สิทธิของผู้ดูแลระบบงานนั้น ๆ มาก่อน ซึ่งสามารถป้องกันได้หลายวิธี อันได้แก่ การกำหนดรหัสผ่านที่ซับซ้อน (Password Policy) แยกสิทธิของผู้ใช้งานออกเป็นหลายระดับ แต่วิธีการที่ดีที่สุด คือการ “ห้ามผู้ใช้งานลงโปรแกรมใด ๆ โดยไม่ได้รับอนุญาต” เนื่องจากผู้ใช้งานทั่วไป (Common User) มีเป็นจำนวนมาก และมักมีความตระหนักในความปลอดภัยของระบบงาน (Awareness) น้อยกว่าผู้ดูแลระบบ จึงตกเป็นเหยื่อของการโจมตีได้ง่ายและไม่รู้ตัว โดยเฉพาะการใช้โปรแกรมละเมิดลิขสิทธิ์ (Unlicensed) ที่มักจะไม่สามารถทำการปรับปรุงช่องโหว่ด้านความปลอดภัย (Security Patch) จากผู้ผลิตได้สมบูรณ์ ทำให้เกิดช่องโหว่ถาวรอยู่ตลอดเวลา แต่การดำเนินการเช่นนี้มักส่งผลกระทบต่อความพึงพอใจของผู้ใช้งานที่มักต้องการอิสระ จึงจำเป็นต้องกำหนดเป็นนโยบายภาพรวมให้ทั้งองค์กรรับทราบทั่วกัน

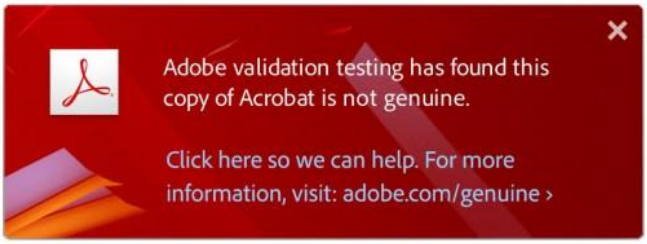


*Figure 6: Software ละเมิดลิขสิทธิ์กลุ่ม Adobe ซึ่งมีความเสี่ยงสูงมาก*[4]

5. **<u>การดูดข้อมูล(Exfiltrate)</u>**

เมื่อผู้โจมตีสามารถเพิ่มสิทธิตัวเองให้เทียบเท่าผู้ดูแลระบบ (Administrator/Root) ได้แล้ว ขั้นตอนที่จำเป็นต่อไป คือ หาวิธีส่งกลับข้อมูล (Exfiltrate/Retrieve Data) สำคัญของเหยื่อไปยังส่วนที่ตนเองสามารถเข้าถึงได้ง่ายในภายหลัง แทนที่จะต้องเริ่มกระบวนการโจมตีใหม่ทุกครั้ง เพื่อเข้าถึงข้อมูลดังกล่าว โดยสามารถทำได้หลายกรณีทั้งทางกายภาพ (Physical) เช่น การสำเนาข้อมูลใส่ USB - Drive แล้วนำออกมาจากสถานที่นั้น หรือใช้สิทธิผู้ดูแลระบบ (Admin) ปิดระบบรักษาความปลอดภัยต่าง ๆ (เช่น IDS, Firewall) เป็นการชั่วคราว เพื่อเปิดช่องทางส่งข้อมูล (Protocol) แบบต่าง ๆ เช่น FTP (File Transfer Protocol) หรือ SCP (Secure Copy Protocol) โดยปะปนกับข้อมูลทั่วไปที่ระบบงานนั้น ๆ มีการส่งเป็นประจำอยู่แล้ว

แนวทางการป้องกัน

ในกรณีที่ผู้โจมตีได้เข้าถึงระบบภายในแล้วการป้องกันดูดข้อมูลจะเป็นไปได้ยาก แต่วิธีการรับมือ (Countermeasure) ที่เป็นไปได้คือ ผู้ดูแลระบบต้องคอยตรวจสอบประวัติการทำงาน (History Log) ของระบบป้องกันภายในองค์กรอย่างสม่ำเสมอว่ามีพฤติกรรมผิดสังเกตหรือไม่ พร้อมทั้งคอยตรวจสอบสิทธิการใช้งานของ (User Privilege) ว่าเป็นไปตามที่กำหนดก่อนล่วงหน้ารึเปล่า เพื่อหยุดยั้งการส่งข้อมูลออกไปสู่ภายนอก

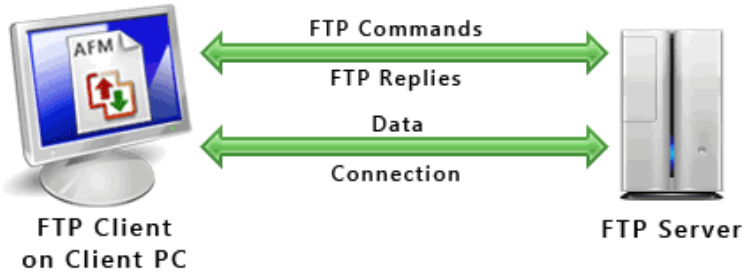


*Figure 7: การรับส่งข้อมูลผ่าน FTP Protocol*[5]

6. **การโจมตี(Assault)**

เมื่อได้รับข้อมูลที่จำเป็นแล้ว ขั้นตอนถัดไปคือการใช้ประโยชน์จากระบบงานนั้น ๆ ตามวัตถุประสงค์หรือทำลายระบบดังกล่าวให้ไม่สามารถใช้งานได้ตามปกติ โดยมีแนวคิดในการโจมตีทางไซเบอร์อยู่ 5 ประการ ได้แก่

- การลวง (Deception)

เป็นการป้อนข้อมูลอันเป็นเท็จให้กับฝ่ายตรงข้าม เพื่อให้มีการดำเนินการตัดสินใจที่ผิดพลาดไม่ตรงกับข้อเท็จจริง เช่น กรณีที่ผู้โจมตีสามารถแฮคเข้าระบบควบคุมการยิง(คคย.) หรือระบบสื่อสารผ่านวงจร (VOIP: Voice over Internet Protocol) ของหน่วยรบในพื้นที อาจจะทำการส่งคำสั่งยิงลวง หรือพิกัดยิงที่ผิดพลาดให้กับหน่วยยิงสนับสนุนทำการโจมตีแบบมีอันตรายใกล้ฝ่ายเดียวกัน หรือเปิดเผยที่ตั้งข้าศึกที่ไม่มีจริงเพื่อให้เกิดความสับสนในการเคลื่อนกำลังรบได้เป็นต้น

- การขัดขวาง (Disruption)

เป็นการทำให้ระบบงานของฝ่ายตรงข้ามประสบปัญหาในการทำงาน เช่น ช้า (Delay) หรือความแม่นยำคลาดเคลื่อนได้เป็นต้น เช่นระบบการคำนวนเส้นทาง (Navigation) เพื่อให้ประสิทธิภาพการดำเนินกลยุทธ์หรือวางแผนตกลงกว่าที่ควรจะเป็น

- การปฏิเสธการให้บริการ (DoS: Dinal of Service)

เป็นการโจมตีในรูปแบบที่ทำให้ระบบนั้นใช้การไม่ได้โดยสมบูรณ์เป็นระยะเวลาหนึ่ง ด้วยการส่งข้อมูลขยะจำนวนมหาศาล (Flood) เข้าไปยังช่องทางสื่อสารเดียวกันจนเกินกว่าที่ระบบจะรับได้ ทำให้ข้อมูลที่สำคัญจริงต้องรอเวลาไปเรื่อยๆอย่างไม่มีกำหนดจนถูกบังคับให้ยุติการเชื่อมต่อ (Timeout) โดยปริยาย เช่น การโจมตีเว็บไซต์ที่ให้บริการทางสาธารณะ บริการศูนย์ข้อมูลแลกเปลี่ยนด้านต่าง ๆ เป็นต้น

- การลดทอน (Degradation)

เป็นการทำให้ประสิทธิภาพโดยรวมของระบบลดลง เช่น การโจมตีเครือข่ายภายในบางส่วน ทำให้มีผลกระทบต่อภาพรวม เช่น เกิดปัญหาคอขวด (Bottleneck) หรือบีบบังคับให้ระบบงานต้องไปประมวลผลซ้ำซ้อนในสิ่งที่ไม่จำเป็น (Loop Data) ตัวอย่างในการทหาร เช่น การปิดกั้นโครงข่ายยุทธการ จนบีบให้ระบบงานต้องใช้เส้นทางสำรอง (Backup Link) ซึ่งมีประสิทธิภาพไม่เทียบเท่าเส้นทางปกติ

- การทำลาย (Destruction)

เป็นการทำลายทรัพย์สินโดยตรงของระบบไซเบอร์ ซึ่งเป็นไปได้ทั้งการทำลายข้อมูล (Data) ระบบงานที่ใช้ (Application) ระบบปฏิบัติการ (OS) หรือแม้แต่การทำให้อุปกรณ์ (Physical Hardware) พังเสียหายโดยสมบูรณ์ เช่น กรณีไวรัสสตักซ์เน็ต (Stuxnet) ที่ทำลายเตาปฏิกรณ์นิวเคลียร์ของอิหร่าน หรืออากาศยานไร้คนขับ (UAV) แบบ RQ - 170 Sentinel ของสหรัฐอเมริกาที่ถูกโจมตีทางไซเบอร์ให้ลงจอดในสนามบินของอิหร่าน เป็นต้น

<u>แนวทางการป้องกัน</u>

เมื่อการโจมตีทางไซเบอร์ (Cyber Attack) เริ่มขึ้น ผู้ดูแลระบบจำเป็นต้องตรวจสอบระบบของตนเองโดยละเอียดทันที พร้อมกับประสานงานไปยังผู้ดูแลระบบข้างเคียงเพื่อจำกัดวงความเสียหาย โดยขึ้นกับรูปแบบการโจมตีดังกล่าว ซึ่งการป้องกันสามารถทำได้บางส่วนโดยการย้ายระบบงานไปยัง Backup Site หรือประกาศใช้งานศูนย์ข้อมูลสำรองภาวะวิกฤติ (DR-Site: Disaster Recovery Site) แล้วเริ่มทำการสแกนช่องโหว่ของระบบงานตนเองเพื่อปิดกั้นการโจมตีโดยทันที (Patching)

*Figure 8: ภาพจำลองการโจมตี DoS Attack ต่อ USA*[6]

### 7. การคงอยู่ (Sustain)

ในกรณีที่สามารถเข้าถึงระบบงานและได้สิทธิสูงสุดแล้ว ผู้โจมตีก็มีทางเลือกเพิ่มเติมที่จะปรับแต่งระบบของเหยื่อ (Victim) เพิ่มเติมเพื่อเปิดช่องทางลับพิเศษ (Backdoor) ไว้ให้สามารถเข้าใช้งานระบบอีกครั้งในอนาคต เนื่องจากว่าแม้จะค้นพบกระบวนการโจมตีเข้ามาได้แล้ว แต่ก็มีความเป็นไปได้เช่นกันว่าผู้ดูแลระบบตัวจริงอาจค้นพบช่องโหว่ดังกล่าวและปิดกั้นเสียในภายหลัง (Update Patching) ซึ่งความยากในกระบวนการเหล่านี้ คือ จะทำอย่างไรให้ช่องทางลับพิเศษที่สร้างขึ้นไม่ถูกตรวจพบโดยง่าย ดังนั้น ผู้โจมตีจำเป็นต้องศึกษาโครงสร้างภายในของระบบงานอย่างละเอียดเพื่อจะได้แทรกโปรแกรมดังกล่าวไว้โดยไม่ให้เหยื่อรู้ตัว

วิธีการหนึ่งที่ผู้โจมตีมักใช้เพื่อเพิ่มโอกาศในการคงอยู่ คือ การวางโปรแกรมที่เป็นอันตราย (Malware) ไว้ยังเครื่องของผู้ใช้บริการที่อยู่นอกระบบงาน (User'Machine) แต่เป็นเครื่องที่มีการรับส่งข้อมูลกับเครื่องแม่ข่ายของระบบงานอย่างสม่ำเสมอ ซึ่งแม้ว่าผู้ดูแลระบบจะปิดกั้นช่องโหว่ไปแล้ว แต่ผู้โจมตีก็ยังมีโอกาศในการอาศัยเครื่องมือที่อยู่ภายในองค์กรนั้น ๆ ลักลอบเข้าดำเนินการจู่โจมทางไซเบอร์ได้อย่างต่อเนื่อง

<u>แนวทางป้องกัน</u>

การคงอยู่ของการโจมตีทางไซเบอร์นั้น ไม่มีภัยคุกคามซึ่งหน้าชัดเจน (Non-incident) แต่มีความเสี่ยงอยู่เสมอที่จะถูกโจมตีได้ การป้องกันที่เหมาะสม คือ การกำหนดนโยบายด้านความปลอดภัยโดยเคร่งครัดและมีการตรวจสอบสื่อข้อมูล (PC, Laptop, Smartphone หรือ USB Drive) ที่ใช้ในการเชื่อมต่อกับระบบงานอยู่เสมอพร้อมทั้งผู้ดูแลระบบจะต้องคอยประสานกับระบบงานข้างเคียงที่มีการแลกเปลี่ยนข้อมูลกันให้มีการปรับปรุงความปลอดภัย (Security Patching) ให้สอดคล้องกันด้วย

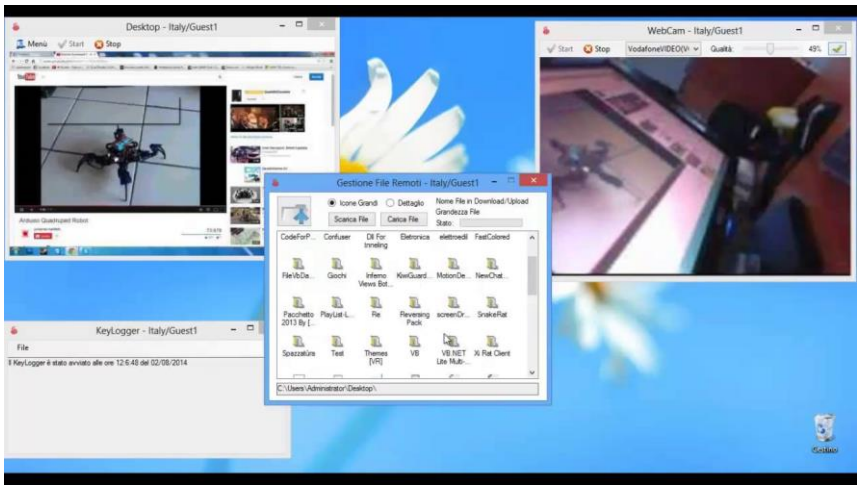


*Figure 9: Software Backdoor ที่แอบดูพฤติกรรมของเหยื่อ*[7]

8. **<u>การซ่อนพราง(Obfuscate)</u>**

เป้าหมายสูงสุดตั้งแต่ขั้นตอนแรกจนถึงขั้นตอนสุดท้ายของการโจมตีทางไซเบอร์ นั่นคือ การกลบร่องรอยในการกระทำของผู้โจมตี (Hacker) หรือทำให้สับสนในแหล่งที่มาเพื่อที่จะป้องกันการสืบสวนแกะรอยทางไซเบอร์ย้อนหลัง (Cyber Forensic) มายังผู้โจมตี โดยมีเป้าหมายว่า *เหยื่อจะต้องไม่รู้ตัวว่ามีอะไรเกิดขึ้น* หรือถึงรู้ก็ไม่สามารถสืบหาสาเหตุหรือแหล่งที่มาของการโจมตีได้

วิธีการที่ง่ายและเป็นที่นิยมสูงสุดของเหล่าแฮคเกอร์ คือ การปกปิดหลักฐานก่อนมายังที่อยู่ทางกายภาพ เริ่มตั้งแต่กระบวนการลาดตระเวณ (Recon) ขั้นแรก ว่าผู้โจมตีจะทำการรวบรวมข้อมูลผ่านตัวกลางที่ไม่เปิดเผย (Proxy) ซึ่งอาจเป็น เว็บไซต์ที่ให้บริการแฮคเกอร์ด้วยกัน หรือเหยื่อผู้ใช้งานทั่วไปที่ติดมัลแวร์ (Zombie) และเป็นฐานให้ทำการจู่โจมบุคคลที่ 3 โดยไม่รู้ตัว พร้อมทั้งซ่อนพรางหมายเลขที่อยู่ของตนเอง (IP-Spoofing) ซึ่ง ยิ่งมีการใช้งานกระบวนการซ่อนพรางเหล่านี้มากเท่าไหร่ ยิ่งทำให้ฝ่ายตั้งรับค้นหาแหล่งที่มาได้ลำบากขึ้นเท่านั้น รวมถึงสามารถใช้เพื่อใส่ร้ายและป้ายความผิดให้กับบุคคลอื่นที่เป็นเหยื่อลำดับถัดไปได้อีกด้วย

<u>แนวทางการป้องกัน</u>

ในกระบวนการซ่อนพรางของแฮคเกอร์นั้น สามารถมีการปกปิดหลายได้หลายชั้นจริง แต่ในขณะเดียวกัน กระบวนการสืบสวนทางไซเบอร์ก็สามารถแกะรอยได้เช่นกัน ในกรณีที่พบเครื่องเป้าหมายที่ถูกโจมตีไว้แล้วและยังไม่เกิดความเสียหายรุนแรง (ระยะฝังตัว) ผู้ดูแลระบบ (Administrator) ที่มีทักษะด้านการสืบสวน (Forensic) สามารถแกะรอยย้อนทางกลับได้เช่นกันเนื่องจากผู้โจมตีก็ไม่รู้ตัวว่าถูกค้นพบแล้ว โดยขั้นตอนหลัก คือ *“อย่าพึ่งปิดเครื่องเป้าหมาย”* เพื่อป้องกันมัลแวร์หลบหนีออกจากเครื่องไป (มัลแวร์หลายตัวจะมีระบบทำลายตัวเองเมื่อถูกตรวจพบ) และเปิดโอกาศให้ผู้เชี่ยวชาญวิเคราะห์มัลแวร์ว่า ส่งข้อมูลย้อนกลับไปที่ใด และแกะรอยย้อนกลับไปเป็นลำดับ

*Figure 10: Lab ของหน่วยสืบสวนดิจิตอลที่แกะรอย Hacker ผ่าน Hardware ของเหยื่อ*[8]

**สรุป**

การปฏิบัติการโจมตีเครือข่ายคอมพิวเตอร์ในปัจจุบันได้มีพัฒนาการเป็นลำดับและรุนแรงขึ้นอย่างต่อเนื่องตามการขยายตัวของระบบสารสนเทศที่มีการใช้งานในทุกองค์กรและแทบทุกองคาพยพ อันเป็นเป้าหมายสำคัญ (High Value Target) ทั้งในด้านการทหารและพลเรือน ซึ่งกองทัพในปัจจุบันเริ่มมียุทธศาสาตร์ปรับเปลี่ยนรูปแบบการปฏิบัติการให้มีการใช้เครือข่ายเป็นศูนย์กลางมากขึ้นเรื่อย ๆ และมีประโยชน์ในการดำเนินกลยุทธ์อย่างยิ่ง แต่พร้อมกันนั้น ก็เป็นช่องโหว่หรือจุดอ่อนที่ฝ่ายตรงข้ามอาจแสวงประโยชน์ได้ โดยเฉพาะอย่างยิ่งการที่อาวุธไซเบอร์นั้นยากต่อการเปิดเผยตัวตน ไม่แสดงผู้รับผิดชอบชัดเจน ขอบเขตการปฏิบัติการกว้างไกลแทบไม่มีจำกัด ทำให้ได้รับความนิยมอย่างมากจากผู้ก่อการร้าย หรือรัฐชาติที่ต้องการจู่โจมฝ่ายตรงข้ามโดยไม่แสดงตัวตน เพื่อใช้เป็นอาวุธทั้งทางด้านการเมืองและการทหารอย่างยิ่งยวด

การรบในปัจจุบันจึงจำเป็นต้องมีการป้องกันและรักษาความปลอดภัยในการปฏิบัติการ เพื่อรักษาความพร้อมรบอย่างเต็มที่ รวมถึงแสวงหาศักยภาพในการทำลายฝ่ายตรงข้ามด้วยอาวุธประเภทเดียวกันเพื่อเป็นการป้องปรามด้วยเช่นกัน

ผู้จัดทำ: ธนรัฐ ธนะสมบูรณ์

ตำแหน่ง: TTA2

**Reference:**

1. NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority 2nd Edition (Revised) by David S. Alberts,John J. Garstka, Frederick P. Stein
2. https://nniwat.wordpress.com/
3. https://www.mozilla.org/en-US/firefox/new
4. https://helpx.adobe.com/security.html
5. http://www.deskshare.com/resources/articles/images/ftp-protocol.gif
6. http://map.norsecorp.com/#/es
7. http://www.tenable.com/sites/
8. http://investigatesc.com/digital-forensics/
9. http://www.deskshare.com/resources/article
10. http://www.pakfiles.com/watch-a7m3d-remote-admin-tool-rat-v3-6355283