ฐิติภัทร จีรภาญจนากร I Network Engineer I Network Consulting Department

รู้ทัน..ป้องกัน กับกลเม็ด การแอบใช้อินเทอร์เน็ตในองค์กร

"เป็นที่หลีกเลี่ยงไม่ได้สำหรับองค์กรในปัจจุบัน ที่จะต้องมีการเชื่อมต่อออกสู่อินเทอร์เน็ต เพื่อให้พนักงานในองค์กรได้ใช้ค้นหาข้อมูล ติดต่อ และทำธุรกรรมต่างๆ แต่มีสักกี่องค์กรที่มีการติดตามและควบคุมการใช้งานให้ถูกต้องตามกฎหมายและคุ้มค่ากับค่าใช้จ่ายที่เสียไป"

[ ] อินเทอร์เน็ตถือว่าเป็นสื่ออิสระประเภทหนึ่งที่นิยมใช้งานแพร่หลายในปัจจุบัน ง่ายต่อการเข้าถึงและสามารถทำได้หลายๆ หน้าที่ได้อย่างสะดวกและรวดเร็ว ไม่ว่าจะเป็นการแสดงความเห็นต่อข่าวสาร การโพสข้อความหรือรูปภาพส่วนตัว ซึ่งเป็นสิ่งที่เห็นชอบด้วยสิทธิส่วนบุคคล รวมไปถึงการรับส่งไฟล์ละเมิดลิขสิทธิ์ สื่ออนาจาร ที่ขัดต่อกฎหมายและศีลธรรมอันดี โดยเฉพาะอย่างยิ่งแล้วการใช้อินเทอร์เน็ตสาธารณะซึ่งยากต่อการควบคุมและติดตามหาบุคคลหากมีการกระทำความผิดเกิดขึ้น ความรับผิดชอบจึงตกเป็นของผู้ให้บริการ หรือผู้ดูแลระบบในองค์กร ซึ่งจะต้องเป็นแรงผลักดันสู่ผู้บริหารองค์กร ให้องค์กรมีการบังคับใช้นโยบายการใช้อินเทอร์เน็ตอย่างถูกต้องและชอบด้วยกฎหมาย บางองค์กรเลือกใช้เครื่องมือทางด้านเน็ตเวิร์กต่างๆ เพื่อเป็นตัวช่วยป้องกันและควบคุมให้พนักงานทุกคนใช้งานอินเทอร์เน็ตให้สอดคล้องกับนโยบายขององค์กรเท่านั้น... แต่อุปกรณ์เหล่านี้ไม่รับประกันว่าจะควบคุมได้ 100% หากขาดการดูแลอย่างใกล้ชิดของผู้ดูแลระบบ

บทความนี้จึงอยากจะแนะนำพฤติกรรมบางพฤติกรรมที่เกิดขึ้นกับผู้ใช้งาน ซึ่งอาจจะเล็ดรอดสายตาของผู้ดูแลระบบไปได้

อินเทอร์เน็ตแรง..โหลด Bittorrent ดีกว่า

Bittorrent หรือที่เรียกกันอย่างติดปากว่า Bit เป็นรูปแบบการแชร์ไฟล์ประเภทหนึ่งที่มีต้นกำเนิดมาจาก Application ประเภท P2P (Peer-to-Peer) ซึ่งสมัยก่อน P2P มีหลักการทำงานแบบหนึ่งต่อหนึ่ง เช่น นาย A แชร์ไฟล์เอาไว้ 1 ไฟล์จากเครื่องคอมพิวเตอร์ของตนเอง นาย B และนาย C ซึ่งเป็นสมาชิกเครือข่าย P2P เช่นกัน ต้องการไฟล์ที่นาย A แชร์ไว้เช่นกัน ก็จะทำการติดต่อโดยตรงกับเครื่องของนาย A เพื่อดาวน์โหลดไฟล์นั้นๆ ลงมาไว้ที่เครื่องของตนเอง แต่การทำการติดต่อทำได้เพียงครั้งละ 1 เท่านั้น หมายความว่านาย B ต้องดาวน์โหลดจนสำเร็จก่อน นาย C จึงจะติดต่อได้ จึงเหมาะกับแชร์ไฟล์ขนาดเล็กๆ เท่านั้น เช่น ไฟล์ MP3 รูป หรือ Zip File แต่ปัจจุบัน Bittorrent ทำลายข้อจำกัดนี้ลง ส่งผลให้ไฟล์หนึ่งๆ หรือเครื่องคอมพิวเตอร์สมาชิกหนึ่งๆ สามารถส่งถ่ายได้หลาย Connection ทำให้มีความรวดเร็วและความถูกต้องที่สูงขึ้น ด้วยวิธีการทำงานที่แตกต่างกันเล็กน้อย เริ่มจากองค์ประกอบต่างๆ ของ Bittorrent ดังนี้

1. **Tracker Client หรือ Bittorrent Client** คือ Application ที่ใช้ในการ Download (Leecher) และ Upload (Seeder) ซึ่งในปัจจุบันมีหลายตัว มีความสามารถที่ต่างกัน จุดนี้เองเป็นจุดที่ผู้ใช้เลือกใช้ตัวที่มีความสามารถในการหลีกเลี่ยงการตรวจจับ ส่งผลให้ผู้ใช้สามารถแอบใช้ Bittorrent ในองค์กรได้

2. **Tracker Server** ทำหน้าที่เก็บรายชื่อของสมาชิกและไฟล์ทั้งหมดที่มีการแชร์ บางแห่งจะทำหน้าเก็บข้อมูลการ Download/Upload ของสมาชิกแต่ละคนด้วย เพื่อเป็นข้อบังคับให้สมาชิกแต่ละคนแชร์ไฟล์ของตัวเองให้ผู้อื่นบ้าง จุดนี้เองทำให้สมาชิกผู้ใช้งานเกิดห่วงโซ่การใช้งานแบนด์วิธด์ นอกจากจะต้องเปลืองแบนด์วิธด์ไปกับการ Download แล้ว ยังต้องเปลืองแบนด์วิธด์ไปกับการ Upload ไฟล์ให้ผู้อื่นด้วย

3. **Tracker File** เป็นตัวแทนของไฟล์ต่างๆ ที่สมาชิกของ Tracker Server ทำการแชร์เอาไว้ เช่น ผู้ที่ทำการแชร์ต้องการแชร์ไฟล์ขนาด 500 MB จากนั้นจึง Publish ข้อมูลขึ้นไปบน Tracker Server จากนั้น Tracker Server จะทำการ Generate Tracker File ที่มีขนาดเพียงแค่ไม่ถึง 100 KB ซึ่งประกอบไปด้วยรายชื่อไฟล์ ขนาดไฟล์ การตรวจสอบความถูกต้อง (Hash) รายชื่อสมาชิกของไฟล์ที่ทำการแชร์ ผู้ที่ต้องการ Download สามารถร้องขอไฟล์นี้จาก Tracker Server เพื่อให้ Tracker Client ทำการติดต่อกับ Tracker Server (ที่ระบุใน Torrent) เพื่อขอรายชื่อผู้ที่อยู่ใน Swarm (กลุ่มผู้ใช้งานที่มีส่วนเกี่ยวข้องกับข้อมูลนั้น) ของไฟล์นั้นๆ ในปัจจุบัน ตัว Tracker จะรู้ว่าสมาชิกของ Swarm มีชิ้นส่วนไหนของไฟล์รวมทั้งสถานะของสมาชิกแต่ละคน หาก Tracker เกิดขัดข้องก็จะไม่สามารถเริ่มโหลดไฟล์นั้นได้ ถ้าการทำงานทั้งหมดถูกต้องก็จะทำการ Download ไฟล์นี้จนสำเร็จ

การทำงานของ BitTorrent จะต้องมีทั้ง 3 ข้อนี้ ถ้าขาดส่วนใดส่วนหนึ่ง โครงข่ายนี้จะไม่สมบูรณ์ทันที และถ้าโครงข่ายของ BitTorrent นี้มีผู้เข้ามาร่วมมากเท่าไหร่ อัตราการ Tranfer File ก็สูงยิ่งขึ้น อีกทั้ง BitTorrent มีความแม่นยำในการดาวน์-โหลดสูงกล่าวคือ เมื่อเราดาวน์โหลดไฟล์ประเภทเพลง หรือหนัง โอกาสที่ไฟล์จะเสียนั้นมีน้อยมากๆ หรือแทบไม่มีเลย เพราะไฟล์ Torrent เป็นตัวเก็บชิ้นส่วนขนาดไฟล์ตัวจริงไว้ แล้วแยกซอยเป็นชิ้นเล็กๆ ทำให้ส่งถ่ายได้แม่นยำ รวมทั้งมีการตรวจสอบไฟล์ทุกๆ ชิ้นที่ส่งถ่ายมาตลอดเวลา

เนื่องจากธรรมชาติของ BitTorrent จะต้องมีการสร้าง Connection หลายๆ Connection เพื่อติดต่อกับ Peer จำนวนมากมายที่ได้รับข้อมูลมาจาก Swarm ใน Tracker **ดังนั้นการโหลดไฟล์จาก BitTorrent จึงมีความเร็วสูง แต่กลับส่งผลเสียต่อองค์กรอย่างมากมาย**

- การโหลดไฟล์ผ่านเครือข่าย BitTorrent นั้นไม่เกี่ยวข้องกับการทำงาน หรือเกี่ยวข้องน้อยมาก
- ไม่สามารถควบคุมความเร็วในการใช้งานได้
- ทำให้ Bandwidth ภายในองค์กรเต็มอย่างรวดเร็ว ส่งผลให้ไม่สามารถใช้งาน Application หลักขององค์กรได้อย่างเต็มประสิทธิภาพ

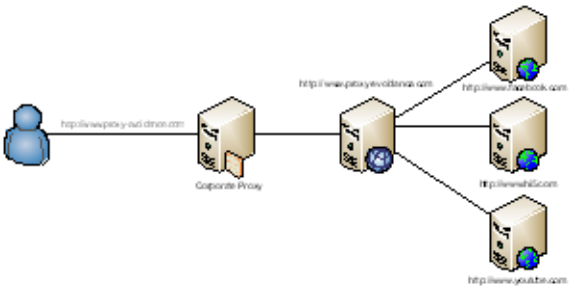
ใช้ Firewall ก็กันได้อยู่แล้ว...แน่ใจหรือ???

เพราะการใช้อุปกรณ์ประเภท Firewall ปิดกั้นการเชื่อมต่อ Port อื่นๆ และอนุญาตให้เชื่อมต่อเฉพาะ Port ที่จำเป็น เช่น 80 (HTTP), 443 (SSL), 20-21 (FTP), 25 (SMTP) ไม่สามารถกีดกันการใช้งาน Bittorrent ได้เพียงพอ Bittorrent Client บางตัวสามารถใช้การเชื่อมต่อผ่าน Port 80 และทำการเข้ารหัส Request Header เพื่อหลบการตรวจสอบของอุปกรณ์ประเภท IDS/IPS อีกด้วย วิธีการป้องกันการใช้งาน Bittorrent ในองค์กรจึงจำเป็นต้องใช้หลายทางร่วมกัน

อีกวิธีหนึ่งซึ่งค่อนข้างจะได้ผลแต่ผู้ดูแลระบบหลายท่านอาจจะมองข้ามไป คือ การใช้งาน Proxy ที่องค์กรใช้งานอยู่ เพราะ Proxy เองเปรียบเสมือน Web Gateway เพราะฉะนั้นถ้าผู้ใช้งานเลี่ยงมาใช้งาน Bittorrent ผ่าน Port 80 แล้วนั้นก็อย่าคิดว่าจะผ่านด่าน Proxy ซึ่งเป็นเหมือนด่านของ Port 80 นั่นเอง โดยที่อย่างน้อย Proxy จะต้องมีความสามารถดังต่อไปนี้

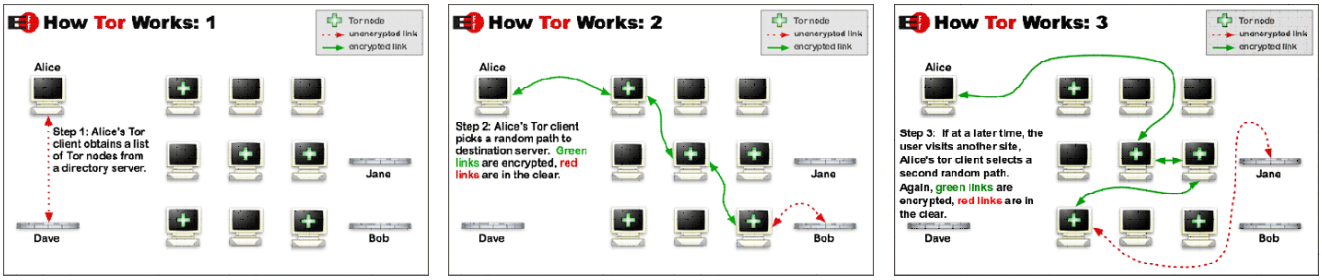
- ตรวจจับและควบคุมการใช้ User-Agent
- ตรวจจับ Protocol Header โดยต้องสามารถทำ Protocol Hand-off ได้ด้วย
- และความสามารถในการจัดกลุ่ม Website (Categories) พร้อมทั้ง Database ที่เชื่อถือได้ในประเทศไทย

เพียงเท่านี้องค์กรก็จะปลอดภัยจากการแอบกระทำความผิดผ่าน Bittorrent แล้ว แต่ยังไม่จบเท่านั้น หลายๆ องค์กรมีการใช้งาน Proxy เพื่อควบคุมการเรียกใช้ Website และเก็บข้อมูลการใช้อินเทอร์เน็ต (Access Log) แล้วแต่หลายครั้งก็เหมือนการควบคุมไม่ได้ผล เพราะผู้ใช้งานก็ยังแอบหาช่องทางเพื่อเรียกใช้งาน Website เหล่านั้นอยู่ดี



แปลกจริงๆ... ทำไม Block Website แล้วยังแอบเล็ดรอดใช้งานได้อีก

ปัจจุบันมีเทคนิคใหม่ๆ ที่ทำให้ผู้ใช้งานที่ใช้งานผ่าน Proxy สามารถหลบเลี่ยงการควบคุมของ Proxy ได้หลายวิธี วิธีหนึ่งที่นิยมใช้คือการใช้งานผ่าน Proxy-Avoidance Website ซึ่งเป็น Website ที่ถูกพัฒนาขึ้นมาเป็นพิเศษ ทำหน้าที่คล้าย Proxy ขนาดย่อม เมื่อผู้ใช้งานต้องการเรียก Website แต่ Website นั้นๆ ถูกปิดกั้นโดย Proxy ภายในองค์กร ผู้ใช้งานเพียงแค่เรียก Website ที่อยู่ในกลุ่ม Proxy-Avoidance



ภาพจาก https://www.torproject.org/overview.html.en#thesolution

แล้วเรียกใช้งาน Website ที่ต้องการเรียกใช้ผ่าน Proxy-Avoidance Website เพียงเท่านี้ Website ที่ผู้ใช้งานต้องการเรียกใช้ก็สามารถเข้าใช้งานได้ โดยผ่าน Proxy-Avoidance Website นั้นๆ เพราะฉะนั้น Proxy ขององค์กรก็จะบันทึกการใช้งานแค่ผู้ใช้งานมีการเรียกใช้ Proxy-Avoidance Website แต่ไม่สามารถรู้ได้เลยว่าจริงๆ แล้ว ผู้ใช้งานเรียกใช้ Website ใด แต่ Proxy ในปัจจุบันมีความฉลาดในการจัดกลุ่มของ Website (Categories) มากขึ้น ก็สามารถช่วยลดปัญหาการเรียกใช้งานกลุ่ม Proxy-Avoidance Website ได้ แทบเรียกได้ว่าเกือบทุก Website เลยทีเดียว

เมื่อไม่นานมานี้เทคนิคใหม่ที่มีชื่อเรียกว่า Tunneling Application เริ่มแพร่หลาย และได้ผลดีกว่า Proxy-Avoidance มาก ซึ่งที่จริงแล้ว Tunneling Application ถูกพัฒนาขึ้นเพื่อความเป็นนิรนามและความเป็นส่วนตัวในอินเทอร์เน็ต โดยมีลักษณะเป็นซอฟต์แวร์ติดตั้งลงที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน และทำงานโดยติดต่อไปที่สมาชิกเครือข่าย (Node) เครื่องอื่นๆ ไปเรื่อยๆ โดยที่ข้อมูลที่โอนถ่ายจะถูกเข้ารหัสที่เยี่ยมยอด ทำให้ Stealth ได้เป็นอย่างดี ทุกๆ Packet ที่ส่งออกไปจะไม่เป็น IP เดียวเลย ทำให้จับต้นชนปลายอะไรไม่ได้เลย

การทำงานของ Tunneling Application ก็จะมีส่วนสำคัญคือ Directory Server ซึ่งจะจัดเก็บรายชื่อสมาชิก (Node) เอาไว้ เมื่อเครื่องคอมพิวเตอร์ของผู้ใช้งานสามารถติดต่อรับรายชื่อ Node กับ Directory Server ได้แล้ว ก็จะทำการเชื่อมต่อโดยมีการเข้ารหัสไปยัง Node ต่างๆ โดยที่กว่าจะถึงเครื่องปลายทางก็จะมีการเชื่อมต่อแบบเดียวกันนี้หลายต่อหลายครั้ง บางครั้งอาจจะมีการเปลี่ยนเส้นทางระหว่างทางด้วย เป็นเหตุผลให้ไม่สามารถติดตามการส่งข้อมูลผ่านเครือข่ายนี้ได้เลย ถ้าเป็นการใช้งานผ่านเครือข่ายขององค์กร ก็จะไม่สามารถติดตามได้ว่าผู้ใช้งานเรียกใช้งานอะไร ฝั่งปลายทางก็จะไม่ทราบว่ามีการเรียกใช้งานจากไหน เรียกได้ว่าสามารถ Stealth ได้ 100%

ยิ่งมีคนร่วมกันใช้ Technique นี้มากเท่าไหร่ ยิ่งเป็น Cellular มากเท่านั้น IP ที่เครื่องปลายทางมองเห็นจึงเป็น IP ของเครื่องสุดท้ายที่ Direct connect จริงๆ ข้อมูลทั้งหมดยังถูกสับออกเป็น Packet เล็กๆ ช่วยกันกระจายออกไปด้วยข้อมูลขนาดเล็กๆ หลายๆ Packet และวิ่งออกไปหลายเส้นทาง ส่งต่อกันหลายทอด และข้อมูลนี้ก็จะไปถึงปลายทาง เป็นที่แน่นอนว่า ถ้าใช้วิธีนี้ในการเรียกใช้ Website ย่อมช้ากว่าการเข้าถึงปกติ ส่วนใหญ่ใช้เวลามากกว่าประมาณ 3-5 เท่าตัว แต่เรียกใช้งานได้แน่นอน ยิ่งถ้าคอมพิวเตอร์เครื่องนั้นสามารถเข้าถึงอินเทอร์เน็ตได้ ไม่ว่าจะเปิด Port ไหนก็สามารถเชื่อมต่อด้วย Technique นี้ได้สำเร็จทั้งสิ้น ยิ่งไปกว่านั้น ถึงแม้เครื่องที่เชื่อมต่อจะไม่มีเส้นทางการเข้าสู่อินเทอร์เน็ตเลย แต่ในอินทราเน็ตมีเครื่องใดเครื่องหนึ่งที่มีการใช้แอพพลิเคชั่นประเภทนี้ มันสามารถทำตัวเป็น Gateway ให้เครื่องอื่นๆ ที่ใช้ Technique นี้ออกสู่อินเทอร์เน็ตได้เช่นกัน

แล้วองค์กรควรจะป้องกันอย่างไรดี????

ถ้าปล่อยให้พฤติกรรมแบบนี้ดำเนินต่อไปในองค์กร จะต้องเกิดผลเสียกับองค์กรอย่างแน่นอน ไม่ว่าจะด้านแบนด์วิธด์ที่เปลืองไปกับ Website ที่มีการลักลอบเรียกใช้ อีกทั้งหากมีการกระทำผิดเกิดขึ้นก็ไม่สามารถที่จะระบุตัวผู้กระทำได้ ความผิดก็จะตกอยู่กับผู้ดูแลระบบและผู้บริหารอย่างหลีกเลี่ยงไม่ได้ ซึ่งเทคนิคแบบนี้ก็จะต้องใช้หลายวิธีร่วมกันในการควบคุม ตัวอย่างเช่น

- อุปกรณ์ประเภท Proxy ที่มีความสามารถในการจัดกลุ่ม Website และตรวจสอบ Request Header รวมไปถึงสามารถทำการ Authentication แบบต่างๆ ที่สามารถช่วยในการป้องกัน Tunneling Application ได้ด้วย
- อุปกรณ์ประเภท Bandwidth Management สำหรับตรวจสอบการใช้งาน Bandwidth ในองค์กร
- รวมไปถึงการหมั่นตรวจสอบเครื่องคอมพิวเตอร์ในสังกัดขององค์กร เพื่อให้มั่นใจว่ามีการติดตั้งชุดซอฟต์แวร์ที่ถูกต้องตามนโยบายขององค์กรนั้นๆ

เพียงรู้เท่าทันพฤติกรรมการใช้งานอินเทอร์เน็ตแบบผิดๆ ในองค์กรแค่นี้ องค์กรของเราก็ปลอดภัยและใช้งานได้เต็มประสิทธิภาพแล้ว โดยถ้าท่านต้องการคำปรึกษาหรือขอข้อมูลเพิ่ม ทางบริษัท TCS มีความยินดี และมีผู้เชี่ยวชาญในการให้คำปรึกษา ที่มีประสบการณ์หลากหลายในทุกกลุ่มตลาดลูกค้า บริษัทชั้นนำ องค์กรต่างๆ โดยท่านสามารถติดต่อได้ที่อีเมล์ thitipat.j@g-able.com

ติดต่อสอบถามข้อมูลเพิ่มเติมได้ที่
บริษัท เดอะ คอมมูนิเคชั่น โซลูชั่น จำกัด
โทร. 0-2685-9333