DDoS

Fight for Availability

หยุดมัน

ก่อนที่มันจะหยุดเรา

Snoc

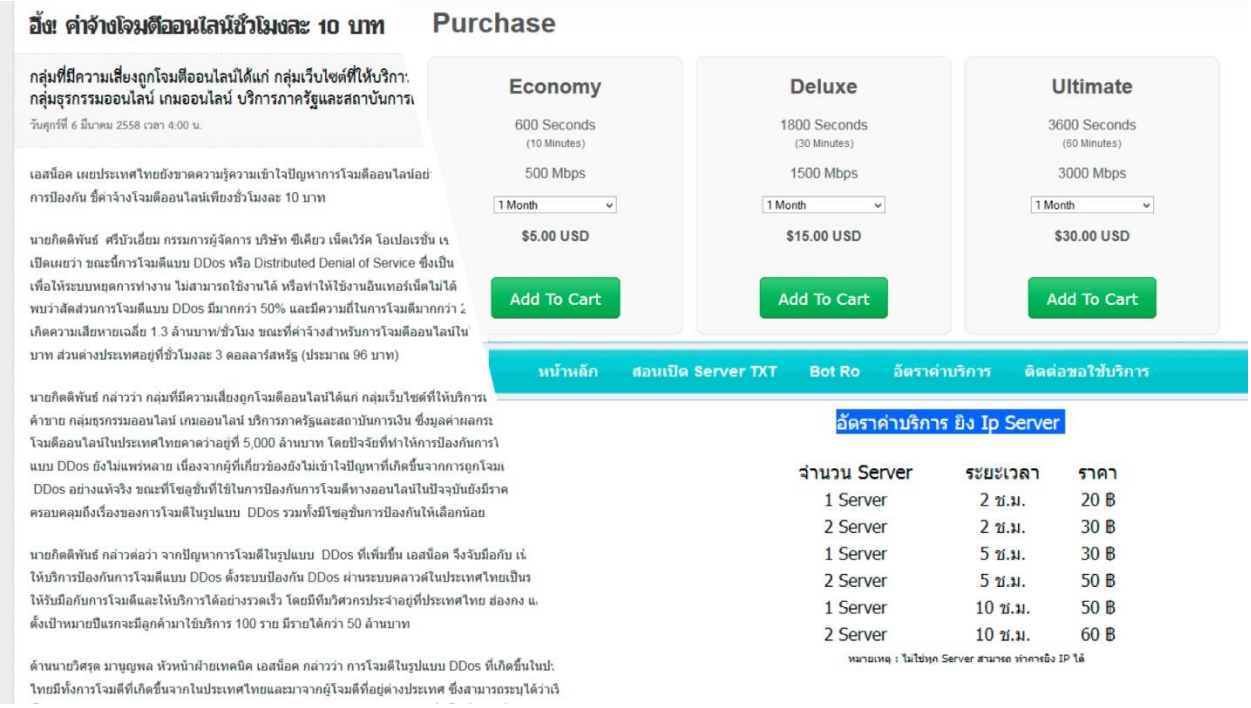
Contents

Chapter 1:

Introduction

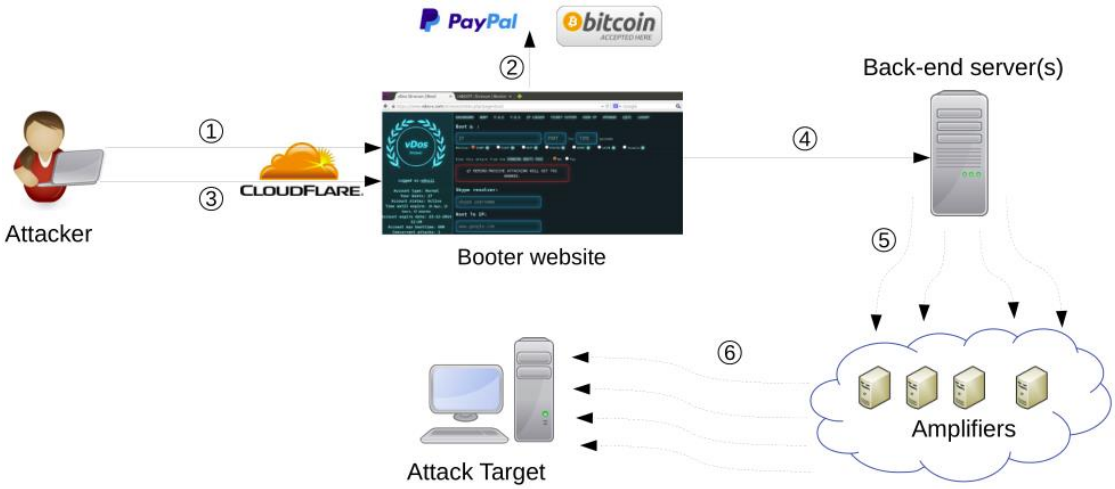
บทความนี้ทางเรามีความตั้งใจในการนำเสนอเคล็ดลับที่จะต่อกรกับ **distributed denial-of-service** หรือ **DDoS** ซึ่งการโจมตีชนิดนี้มีความมุ่งหวังเพื่อทำให้เป้าหมายไม่สามารถให้บริการได้ตามปกติ โดยมักจะมาในรูปแบบ **flooding** ข้อมูลขยะจำนวนมหาศาลจนทำให้ทรัพยากรที่มีอยู่ไม่เพียงพอต่อการให้บริการ ไม่ว่าจะเป็นการทำให้ **Bandwidth Internet, Memory, CPU** เต็มเป็นต้น

การโจมตีด้วย **DDoS** ในปัจจุบันมีช่องทางที่ให้บริการรับจ้างโจมตีหรือบริการทดสอบ **DDoS** ที่เรียกกันว่า **IP Booter, Booter Service และ Stress Testing** มักจะมีอัตราค่าให้บริการก็มีราคาที่ต่ำมากเมื่อเทียบกับ ผลกระทบที่เกิดขึ้นกับธุรกิจ



รูปที่ 1 บริการ DDoS for Hire

รูปแบบการให้บริการส่วนใหญ่จะแฝงตัวเองโดยใช้บริการของ **Cloud Flare** เพื่อเป็นการปิดบังตัวตนจากกฎหมาย คู่แข่ง มีการเรียกเก็บค่าใช้บริการผ่านทางช่องทางของ **Paypal** และ **BitCoin** (หากเป็นผู้ให้บริการในประเทศไทยก็มักจะใช้ ช่องทาง **Online Payment** ชื่อดังร่วมด้วย) โดยผู้ให้บริการรับจ้างโจมตีแต่ละรายก็มีจุดขายที่แตกต่างกันไม่ต่างกับธุรกิจที่ อยู่บนดินทั่วไป เช่น สามารถโจมตีได้ **60Gbps**, สามารถสั่งการได้จากมือถือ, สามารถโจมตีในลักษณะ **Application Base Attack** เป็นต้น



รูปที่ 2 Structure of DDoS service

และที่น่าจับตาในปัจจุบันคือกลุ่ม **DD4BC** หรือ **DDoS for Bitcoin** ที่เรียกค่าไถ่จากเหยื่อโดยจะต้องจ่ายค่าเป็น **Bitcoin** จึงจะหยุดโจมตีด้วย **DDoS** (ดูคล้ายๆกับ **ransomware** เลยใช่ไหมครับ) ซึ่งการโจมตีด้วย **DDoS** โดยส่วนใหญ่แล้วมักจะนิยมใช้ **UDP** ในการโจมตีแต่ก็ยังมีเทคนิคอื่นๆอีก เช่น

- **Reflection / Amplification** ที่อาศัยจุดอ่อนของโปรโตคอลที่นิยมใช้กันแพร่หลายเช่น **DNS,SNMP, SSDP, NTP, RIP (Routing protocol)** ชนิดหนึ่งที่ใช้ในการแลกเปลี่ยนเส้นทางของอุปกรณ์ค้นหาเส้นทาง -- **Router**)
- **L3/L4 Flood** เช่น **Ping of Death, TCP SYN Flood, UDP Fragment**
- **HTTP GET/POST flood**

ดังนั้นแผนที่ใช้รับมือ **DDoS** จึงมีสำคัญ เนื่องด้วยปัญหานี้ไม่สามารถจัดการได้เพียงลำพัง จำเป็นต้องมีการประสานไปยังหลายฝ่ายทั้งภายในและภายนอก และในบางครั้งการโจมตีจะดำเนินไปด้วยระยะเวลายาวนานหลายวัน ซึ่งจำเป็นต้องมีแผนการบริหารบุคลกรให้มีความพร้อมด้วยเช่นกัน

GitHub Status

UPDATED LESS THAN A MINUTE AGO

Status Messages

« Dashboard

August 25, 2015

16:39 ICT	We are investigating reports of connectivity problems.
17:07 ICT	We're continuing to diagnose reports of connectivity problems.
17:38 ICT	The connectivity problems have been identified as a DDoS attack. We're working to mitigate now.
18:06 ICT	We are continuing to work to mitigate an ongoing DDoS attack.
18:27 ICT	We are restoring service as we mitigate a DDoS attack.
19:08 ICT	We are restoring service as we mitigate a DDoS attack. Response times may be slower while this work continues.
19:52 ICT	Service has been restored. We continue to monitor the situation closely.
20:49 ICT	Everything operating normally.

รูปที่ 3 GitHub Status on August 25, 2015

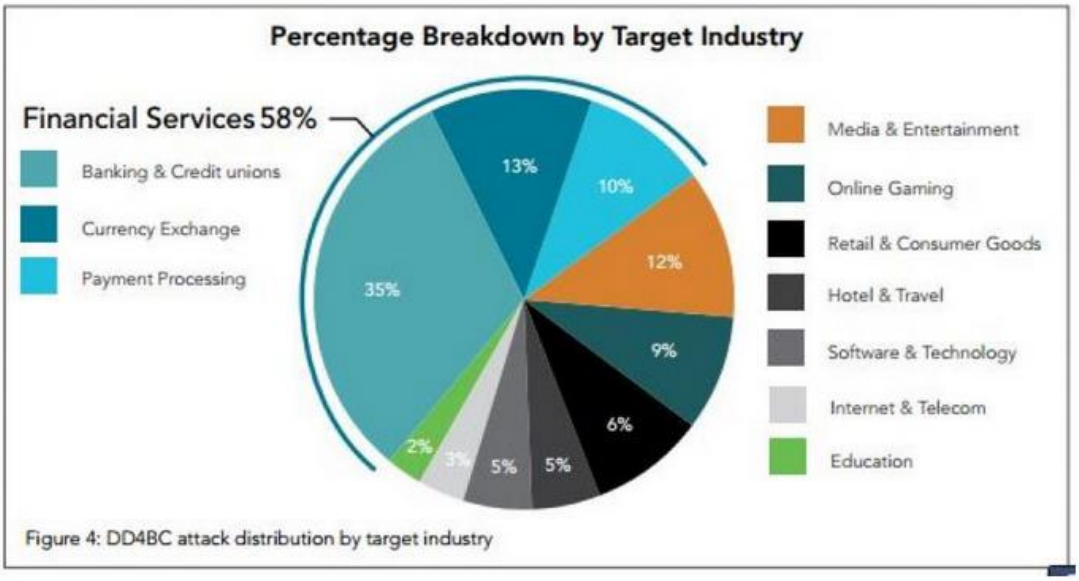


Figure 4: DD4BC attack distribution by target industry

รูปที่ 4 พฤติกรรมของกลุ่ม DD4BC ที่ใช้ DDoS เรียกค่าไถ่

Chapter 2:

Build the DDoS response plan with Checklist

แผนการรับมือประกอบด้วย 3 ขั้นตอนหลักคือ ขั้นตอนเริ่มต้น **(Preparation)**, ขั้นตอนวิเคราะห์ **(Analysis)**, ขั้นตอนบรรเทาผลกระทบ **(Mitigation)** และขั้นตอนการทดสอบ **(Test)**

รูปที่ 5 Build the DDoS response plan with Check

ขั้นตอนเริ่มต้น (Preparation)

ในขั้นตอนนี้เป็นการสร้างความเข้าใจระหว่างทีมผู้บริหาร ผู้ดูแลระบบและทีมของผู้ให้บริการ เพื่อให้ทุกฝ่ายมีความเข้าใจขอบเขต, หน้าที่ที่จำเป็นต้องรับผิดชอบโดยมีขั้นตอนข้อเสนอแนะดังนี้

- รวบรวมรายชื่อผู้เกี่ยวข้องที่มีส่วนได้ส่วนเสียทั้งหมด **(Stakeholder)** เช่น ผู้บริหาร, ผู้ให้บริการอินเทอร์เน็ต **(ISP/IDC)**, ทีมงาน **Network/System/Security/BCP/DR**
- ตรวจสอบระบบที่เชื่อมต่อกับอินเทอร์เน็ตและจัดลำดับความสำคัญ
- ทำความเข้าใจผลกระทบที่จะเกิดขึ้นกับธุรกิจเมื่อเกิดเหตุการณ์ถูกโจมตีจนไม่สามารถให้บริการได้
- สอบถามนโยบายในการจัดการ **DDoS** จากผู้ให้บริการอินเทอร์เน็ต **(ISP/IDC)** โดยคำนึงจากความจุที่สามารถป้องกันได้ **(Capacity)** และความหน่วงที่เกิดจากระบบ **(Latency)**
- กำหนด **White-list** ที่จำเป็นต้องทำการติดต่อเช่น **IP Address, Protocol, Application** เป็นต้น
- ปรับค่า **DNS time to live (TTL)** ให้มีค่าน้อยลงเพื่อให้ลดระยะเวลาการอัพเดทเวลามีการแก้ไข **DNS Record**
- ทำงานร่วมกับทีมงานที่จัดทำแผน **BCP** เพื่อให้มีความเข้าใจในเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต
- จัดทำ **Performance/Utilize Baseline** จาก **Server CPU/Memory, Application Usage, Internet Bandwidth, Intranet Bandwidth**

ขั้นตอนวิเคราะห์ (Analysis)

ในขั้นตอนนี้เป็นการดำเนินการเพื่อให้ระบบมีความพร้อมในการป้องกันอยู่ตลอดเวลา ตรวจจับการโจมตีให้มีความรวดเร็ว ดั่งหลักการของซุนวูที่ว่า รู้เขารู้เรา รบร้อยครั้งชนะร้อยครั้ง เพื่อมิให้เป็นดั่งการวิจัยในต่างประเทศที่มีข้อมูลว่า **“กว่าจะพบว่าถูก DDoS ก็ล่วงเลยไปแล้ว 1 ชั่วโมงและกว่าจะจัดการกับการโจมตีนี้ได้ก็ใช้เวลาไปอีกกว่า 1 ชั่วโมง”** โดยมีทางเราข้อเสนอแนะดังนี้

- ทำความเข้าใจและทบทวนเทคนิคที่ใช้ในการโจมตีอยู่สม่ำเสมอ โดยค้นหาข้อมูลได้จากสถิติการโจมตี
- วิเคราะห์และทบทวนทรัพยากรที่ใช้งานในปัจจุบันว่าเพื่อให้แน่ใจว่าสามารถรองรับการโจมตีได้ เช่น **Router, Switch, Server, Firewall, IPS และ WAF** เป็นต้น
- ใช้เครื่องมือในการตรวจจับ วิเคราะห์และแจ้งเตือน เช่น **Network Analyzer, Network Monitoring**

ขั้นตอนบรรเทาผลกระทบ (Mitigation)

ในขั้นตอนนี้เป็นการดำเนินการเพื่อ **Respond** เหตุการณ์ที่จะเกิดขึ้นได้ทันที โดยมีหลายเทคนิคที่จะช่วยบรรเทาผลกระทบที่จะเกิดขึ้นให้ลดลงหรือสูญเสียน้อยที่สุดโดยมีข้อเสนอแนะดังนี้

- เพิ่มจำนวนเครื่องเซิร์ฟเวอร์หรือความเร็วอินเทอร์เน็ตเพื่อรองรับ **DDoS Traffic** ที่จะโจมตีเข้ามา
- ประสานงานกับทางผู้ให้บริการ **(ISP/IDC)** เพื่อจัดทำระบบหยุดการทำงานของระบบเป็นการชั่วคราวด้วยเทคนิค **Remotely triggered black hole หรือ RTBH**
- **Redirect Traffic** ไปยังผู้ให้บริการเพื่อช่วยกรอง **DDoS Traffic** ด้วยเทคนิค **Routing** หรือ **DNS**
- จัดทำสรุปเทคนิคการโจมตี ความเร็วที่ใช้ในการป้องกันและดำเนินการปรับปรุงให้มีประสิทธิภาพมากขึ้นในครั้งต่อไป

ขั้นตอนทดสอบ (Test)

ในขั้นตอนการทดสอบแผนที่ได้ทำไว้ เป็นสิ่งที่สำคัญมากที่จะทำให้ทีมงานทุกฝ่ายมีความเข้าใจและสามารถตอบสนองได้อย่างรวดเร็วเมื่อมีเหตุเกิดขึ้น โดยมีข้อแนะนำในการทดสอบดังต่อไปนี้

- ดำเนินการทดสอบโดยไม่มีการโจมตีจริง โดยยกเหตุการณ์จำลองมาดำเนินแผนที่ได้วางไว้ยกตัวอย่าง เช่น เว็บไซต์ที่ติดตั้งภายในองค์กรถูกโจมตีด้วย **Bandwidth** ขนาด **10Gbps** เป็นต้น
- ทดสอบด้วยตนเองโดยติดตั้งเครื่องที่มีประสิทธิภาพและมีความเร็วอินเทอร์เน็ตที่สูง และโจมตีจากเครื่องมือที่ใช้ทดสอบระบบ เช่น **hping, HOIC, LOIC** เป็นต้น
- ดำเนินการทดสอบด้วยผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัย
- ประเมินผลการทดสอบและนำกลับไปปรับปรุงการทำงาน

เกี่ยวกับเรา

เอสน็อค (Snoc) ในฐานะผู้ให้บริการด้านการรักษาความปลอดภัย เรามีความพยายามในการนำเอาเทคโนโลยีเพื่อต่อสู้และป้องกันการโจมตีทาง Cyber ซึ่งถูกพัฒนาอยู่ตลอดเวลา เพื่อให้ธุรกิจดำเนินไปด้วยความราบรื่น มั่นคงปลอดภัยและมีความเชื่อมั่นจากลูกค้าที่มาใช้บริการ

เรามีผู้เชี่ยวชาญและห้องปฏิบัติการ (SOC) ตั้งอยู่ทั้งในและต่างประเทศ เพื่อตรวจสอบและวิเคราะห์การโจมตีรูปแบบใหม่ๆ ที่จะเกิดขึ้นตลอดเวลา ซึ่งจะคอยช่วยเหลือ (Support), ให้คำที่ปรึกษา (Consult) และคอยป้องกันการโจมตี (incident response) ตลอด 24 ชั่วโมง

How do you know when they DDoS you!

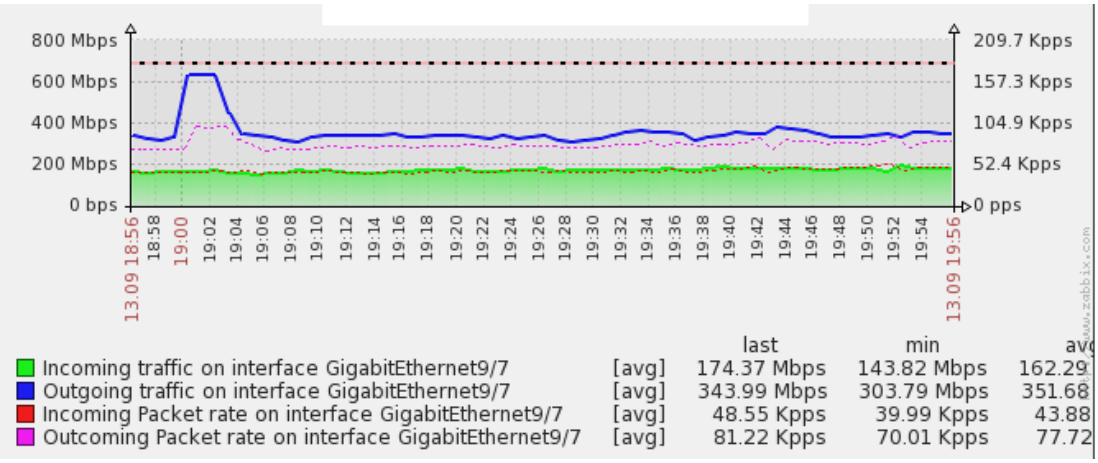
มีรายงานจากทางต่างประเทศเผยตัวเลขกว่า 45% ใช้เวลามากกว่าหนึ่งชั่วโมงกว่าจะรู้ว่าถูกโจมตีด้วย DDoS และใช้เวลาอีกกว่าหนึ่งชั่วโมงกว่าจะจัดการกับปัญหาที่เกิดขึ้น แต่ทางเราเชื่อว่าถ้ามีเครื่องมือและระบบแจ้งเตือนก็สามารถที่จะตรวจพบและตอบสนองกับการโจมตีนี้ได้ไวมากขึ้น

1. Network Monitor เช่น CACTI/ Zabbix / Smokeping

ซอฟแวร์กลุ่มนี้เอาไว้เก็บสถิติการใช้งาน Bandwidth ของเราเตอร์และสวิตซ์ โดยตำแหน่งที่ต้องเฝ้าระวังเป็นพิเศษคืออุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตที่ทำหน้าที่เป็น EDGE โดยดำเนินการดังนี้

- ปรับให้เป็น Real time อัพเดททุกๆ 30 วินาที
- ตั้งค่าความเร็วที่คาดว่าผิดปกติ (Threshold) ยกตัวอย่าง เช่น หากพบว่ามีการใช้งานมากสุดเพียง 350 Mbps ก็ให้ตั้งค่า Threshold ไว้ที่ 400Mbps
- เมื่อพบว่าถึงเกณฑ์ที่ตั้งไว้ก็สามารถแจ้งเตือนเลย

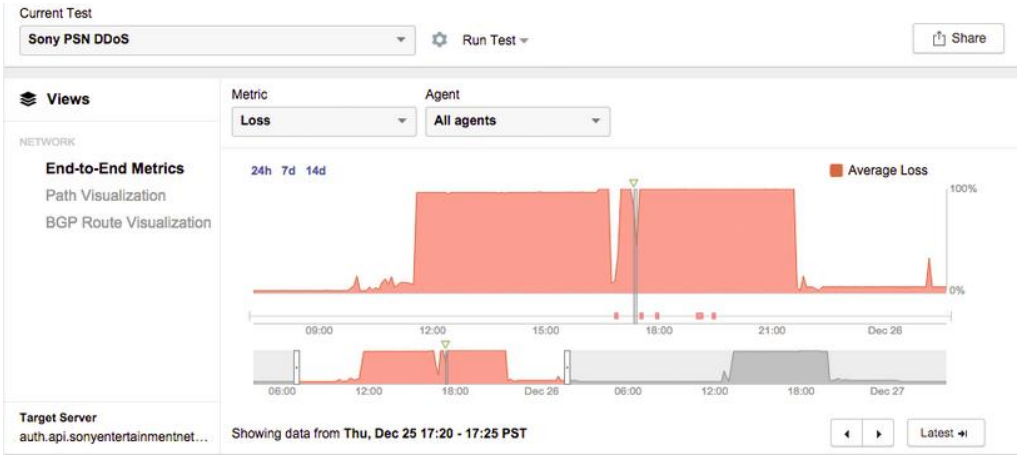
หรือสำหรับท่านที่จำเป็นต้องดูแลเครื่องเซิร์ฟเวอร์ด้วยก็ใช้ความสามารถของ Host monitoring ด้วย Ping, TCP Ping หรือ HTTP Health check เข้าร่วมได้เช่นกัน ซึ่งเมื่อพบว่า Bandwidth มีค่าที่สูงผิดปกติพร้อมกับมีอาการ Packet Loss หรือ HTTP response error ก็สามารถ Mitigation ได้เลย



จากตัวอย่างทำให้ทราบว่ามีสิ่งผิดปกติเกิดขึ้นในช่วง 19.00-19.04 เนื่องจากมี Outgoing traffic และ Packet rate สูงผิดปกติ

2. Thousand Eyes, Site24x7

หากไม่ต้องการติดตั้งซอฟแวร์ตามข้อด้านบนด้วยตนเองให้ยุ่งยาก ก็ต้อง Thousand eyes เพราะว่าสามารถ Monitor BGP และสามารถ Import เข้า Virtual Machine ในระบบของเราแล้วเชื่อมต่อกับ Cloud ของ Thousand eyes ก็ได้ข้อดีของการใช้ บริการนี้คือเป็นการ Monitor แบบ Outside-in ทำให้มองภาพการใช้งานของเรา จากภายนอกได้ตลอดเวลา https://www.thousandeyes.com/solutions/ddos



3. NetFlow/Sflow/Jflow collector

สิ่งที่ทำให้เรารู้ว่าเป็น DDoS หรือไม่ ต้องรู้ก่อนเลยว่า Baseline ของระบบเราคืออะไรและสื่อสารกันด้วยโปรโตคอลอะไรบ้าง ในปัจจุบันนี้สวิตช์ ยังสามารถ export flow ออกมากันได้เลยนะ ถ้าถามว่าจำเป็นไหมส่วนตัวทางผมคิดว่าจำเป็น เพราะในการวิเคราะห์ปัญหาเรื่อง DDoS มีเพียงแค่ Firewall Log อาจจะยังไม่เพียงพอ ซึ่งประโยชน์ของตัวนี้คือจะทำให้รู้ว่าเป้าหมายที่ถูกโจมตีเป็นใคร? จะได้แก้ไขได้อย่างทันท่วงทีส่วนโดยซอฟแวร์ก็มีทั้ง free trial, open source หรือของคนไทยก็มีทำเป็นของ Netka System (สนับสนุนคนไทยด้วยกันหน่อย http://netkasystem.com/)

สรุปท้ายบท

ส่วนกลยุทธ์ที่แนะนำมาทั้งหมดใช้คือใช้ Network Monitoring ทำหน้าที่ตรวจสอบความผิดปกติของ Bandwidth Internet และใช้ตัว Flow Collector/Host Monitoring เป็นตัวเจาะจงว่าระบบใดถูกโจมตี เพียงเท่านี้ก็ลดเวลาที่ใช้ในการตรวจจับได้ไม่น้อยกว่า 50% แต่เหนืออื่นใดจำเป็นต้องฝึกฝนตลอดเวลาเพื่อให้สามารถใช้งานเครื่องมือได้อย่างคล่องแคล่วด้วยครับ

DDoS Mitigation Technique

เทคนิคที่ใช้ป้องกันแบบไหนเหมาะสำหรับคุณ แต่ละแบบแตกต่างกันอย่างไร ป้องกันอะไรได้บ้าง วันนี้เอสน็อคนำมาเปิดเผยกัน 3 เทคนิคด้วยกันคือ

1. RTBH หรือ Remotely Triggered Black hole หรือ Null0

วิธีนี้ใช้เทคนิคที่อยู่บนอุปกรณ์เน็ตเวิคเช่น **Router/Switch** ที่มีความสามารถในการ **drop traffic** ด้วยคำสั่ง **ip route x.x.x.x/32 null 0** ซึ่งผลลัพธ์ก็คือปิดกั้นทราฟฟิคทั้งหมดที่โจมตีมายังปลายทางของเรา ตัวอย่างเช่น **Web server** ของเรามีไอพี **1.2.3.4** เมื่อเราทำ **RTBH** จะส่งผลทำให้ ทราฟฟิคทั้งหมดจะไม่สามารถติดต่อกับ **1.2.3.4** ได้ ย้ำนะครับว่าทุกทราฟฟิค ทุกทราฟฟิค ทุกทราฟฟิค และการที่จะทำ **RTBH** ให้ได้ผลก็คือต้องให้ผู้ให้บริการอินเทอร์เน็ตช่วยทำด้วยเช่นกัน โดยเทคนิคก็คือประกาศผ่านทาง **BGP session** ให้ทำการดรอปทราฟฟิคที่ได้ประกาศออกไป วิธีนี้ฟรีไม่มีค่าใช้จ่ายสามารถติดต่อผู้ให้บริการได้โดยตรง

2. On premise

คือการติดตั้งอุปกรณ์ไว้เพื่อป้องกันการโจมตีโดยอุปกรณ์ที่นิยมใช้ป้องกันก็เช่น

- **Firewall** แต่ด้วยการทำงานที่ถูกออกแบบมาเป็น **Stateful** ทำให้ในบางครั้งเวลาโดน **DDoS** โจมตีหนักๆก็ทำให้เกิดอาการรวนได้เนื่องจากทรัพยากรไม่เพียงพอ
- **DDoS Defense System** เป็นอุปกรณ์ที่ป้องกันโดยเฉพาะ โดยส่วนใหญ่จะทำงานเป็น **Stateless** เลยทำให้ประมวลผลได้ไวกว่าไฟวอลมาก โดยสามารถติดตั้งได้ทั้งรูปแบบวางขวาง **Inline** หรือเป็นแบบภายนอก **Out of band**

แต่เหนือสิ่งอื่นใดสิ่งที่ต้องมีควบคู่กับการติดตั้งแบบ **On premise** คือต้องมี **Bandwidth Internet** จำนวนมากและเพียงพอเพื่อไม่ทำให้เกิดคอขวดด้วยเช่นกัน

3. DDoS Mitigation Service

กลุ่มนี้เป็นผู้ให้บริการป้องกันการโจมตี DDoS โดยเฉพาะ บริการประเภทนี้มีจุดเด่นคือคือค่าใช้จ่ายค่อนข้างต่ำเมื่อเทียบกับการลงทุนเพิ่มความเร็วในการเชื่อมต่ออินเทอร์เน็ตให้เพียงพอต่อการโจมตี ซึ่งในความเป็นจริงเป็นไปได้ยากที่จะสามารถเช่าอินเทอร์เน็ตขนาด 10Gbps มาเพื่อป้องกัน DDoS ซึ่งค่าใช้จ่ายในการต้องจัดหาอินเทอร์เน็ต อาจจะมีค่าใช้จ่ายมากกว่าความเสียหายที่จะเกิดขึ้น โดยวันนี้ทางเอสน็อคจะอธิบาย 2 Solution ที่ผู้ให้บริการสามารถให้บริการได้ดังนี้

- **Scrubbing center with GRE/Direct connected**

  ประเภทนี้สามารถป้องกันได้เกือบทุกระบบโดยใช้เทคนิคการเลือกเส้นทางของ BGP หรือ Border Gateway Protocol ซึ่งการทำงานคือเมื่อพบว่าถูกโจมตีด้วย DDoS จะมีการปรับเส้นทางให้เข้าไปกรองยัง Scrubbing center ก่อนที่จะเข้ามายังระบบ และเพื่อให้ได้ผลมากที่สุดคือจำเป็นต้องมี IP Address จำนวน 1 Class C เป็นอย่างน้อย

- **DNS Base DDoS Protection**

  จะทำการป้องกันเว็บไซต์โดยเฉพาะหลักการคือให้ DNS ทำการส่งข้อมูลที่เป็นประเภท HTTP/HTTP เข้ามายัง Scrubbing center ข้อดีคือ ไม่มีผลกระทบเวลาติดตั้งและใช้เวลาสั้นมากในการติดตั้งเพียงแค่แก้ไข DNS record เท่านั้น และนอกจากจะป้องกัน DDoS แล้วผู้ให้บริการจะมีฟีเจอร์เสริม เช่น ป้องกันการโจมตีจาก บอทเนต (Botnet) ป้องกันการแฮค (Web Application Firewall) และการกระจายทราฟฟิคของผู้เข้าใช้งาน (Load Balance) ด้วยเช่นกัน

www.snoc.co.th

Secure Network Operation Center Co.,Ltd.
72 CAT Telecom Tower 18th Fl. Charoen Krung Rd. Bang Rak Bangkok 10500 Thailand
Tel. 0 2690 3999 Fax 0 2690 3999 E-Mail : sales@snoc.co.th