ระบบตรวจจับเครื่องติดมัลแวร์ภายในองค์กร

Infected Computer Detection System

ณัฐนนท์ นาคสุขศรี

สารนิพนธ์นี้เป็นเป็นส่วนหนึ่งของการศึกษา

หลักสูตรวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณะวิทยาการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีมหานคร

ปีการศึกษา 2561

หัวข้อ	ระบบตรวจจับเครื่องติดมัลแวร์ภายในองค์กร Infected Computer Detection System
ชื่อนักศึกษา	ณัฐนนท์ นาคสุขศรี
รหัสนักศึกษา	6017810012
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาความมั่นคงทางระบบสารสนเทศ
ปีการศึกษา	2561
อาจารย์ที่ปรึกษา	ดร.นันทา จันทร์พิทักษ์

บทคัดย่อ

สารนิพนธ์นี้จัดทำขึ้นเพื่อตรวจจับและแจ้งเตือนเมื่อพบเครื่องคอมพิวเตอร์ถูกติดตั้งมัลแวร์ที่อยู่ภายในเครือบริษัท กรุงเทพดุสิตเวชการ จำกัด โดยมีวัตถุประสงค์เพิ่มประสิทธิภาพในการตรวจจับมัลแวร์ที่ถูกติดตั้งภายในเครื่องคอมพิวเตอร์จากของเดิมที่มีอยู่ ซึ่งในปัจจุบันยังไม่ครอบคลุมกับจำนวนคอมพิวเตอร์ที่มีอยู่มาก โดยระบบตรวจจับเครื่องติดมัลแวร์ภายในองค์กรนี้จะเพิ่มความแม่นยำรวดเร็วและครอบคลุมกับจำนวนคอมพิวเตอร์จำนวนมาก ส่งผลให้ช่วยลดผลกระทบที่เกิดจากการถูกติดตั้งมัลแวร์ ช่วยลดการแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ซึ่งหากถูกติดตั้งมัลแวร์นานเท่าไหร่ ยิ่งได้รับผลกระทบนานขึ้นเท่านั้น

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สามารถสำเร็จลุล่วงได้ด้วยดี เพราะได้รับความช่วยเหลือและคำแนะนำจากบุคคลหลายท่าน ข้าพเจ้าขอขอบพระคุณมา ณ ที่นี้

ขอขอบคุณอาจารย์นันทา จันทร์พิทักษ์ ที่สละเวลาอันมีค่าเป็นที่ปรึกษาโครงงาน และได้แนะนำความรู้และสิ่งที่เป็นประโยชน์ในการช่วยปรับปรุงโครงงานค้นคว้าอิสระฉบับนี้ และขอขอบคุณประธานกรรมการสอบงานค้นคว้าอิสระ และคณะกรรมการผู้ทรงคุณวุฒิ ที่ได้สละเวลามาเป็นคณะกรรมการสอบงานค้นคว้าอิสระ ตลอดจนให้ความคิดเห็นที่เป็นประโยชน์ ในการทำให้งานค้นคว้าอิสระฉบับนี้มีคุณค่ามากยิ่งขึ้น

ขอขอบคุณพี่ ๆ เพื่อน ๆ รวมถึงน้อง ๆ ที่ช่วยแนะนำ อธิบาย ช่วยหาวิธีแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้น พร้อมทั้งเป็นกำลังใจที่ดีในการพัฒนาโครงงานนี้จนสำเร็จไปด้วยดี

ณัฐนนท์ นาคสุขศรี

ตุลาคม 2561

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

หน้า

สารบัญรูป (ต่อ)

หน้า

สารบัญตาราง

หน้า

บทที่ 1

บทนำ

1.1 ปัญหาและแรงจูงใจ

ในขณะที่เทคโนโลยีถูกพัฒนาไปอย่างรวดเร็วเพื่อตอบสนองความต้องการของโลกยุคดิจิทัล ข้อมูลกลายเป็นขุมทรัพย์ที่มีมูลค่ามากยิ่งขึ้น ภัยคุกคามไซเบอร์ก็มีวิวัฒนาการเช่นเดียวกัน แฮ็คเกอร์พยายามสร้างมัลแวร์ประเภทใหม่ เพิ่มความซับซ้อน และเสริมเทคนิคหลบหลีกระบบตรวจจับเข้าไปเพื่อขู่กรรโชกและโขมยข้อมูล ทำให้ระบบรักษาความมั่นคงปลอดภัยในปัจจุบันไม่สามารถตรวจจับและรับมือได้ทัน องค์กรต่างๆ มีความเสี่ยงที่จะถูกโจมตีสูงมากขึ้น

หลายๆ องค์กรที่มี Data Center เป็นของตัวเอง ก็เริ่มลงทุนในเรื่องของ Next-Generation Firewall มากขึ้น สำหรับการป้องกันการโจมตีรูปแบบใหม่ๆที่มีการอัพเดตอยู่เสมอ ซึ่งจะมีคุณสมบัติที่ป้องกันการโจมตีอาทิเช่น IPS, Anti-Malwares เป็นต้น ซึ่งการทำงานของ Anti-Malwares บน Next-Generation Firewall จะตรวจสอบจาก Traffic จากเครื่องที่ติด Malwares ที่ติดต่อกับ C&C Server และ DNS Query ไปยัง Domains ของ C&C Server

อย่างไรก็ตาม หากองค์กรมีสาขาจำนวนมาก และแต่ละสาขามี DNS Server ที่ทำ DNS Forwarding มาที่ DNS Server ที่ Traffic ผ่าน Next-Generation Firewall ซึ่ง Log ที่เกิดขึ้นจะเห็นเครื่องที่ติด Malwares เป็นเครื่อง DNS Server ทำให้ไม่พบเครื่องที่ติด Malwares จริงๆ ทำให้ไม่สามารถไปตรวจสอบเครื่องต้นทางที่ทำให้เกิด Alert นี้ขึ้นมา ดังรูปที่ 1

Severity	Receive Time	Type	Name	Attacker	From Port	Victim	To Port
medium	10/23 23:18:38	spyware	Suspicious DNS Query (generic:uqqtflckhuu.biz)	172.18.10.32	58252	203.155.33.2	53
medium	10/23 23:18:28	spyware	Suspicious DNS Query (generic:lyvimje.net)	172.18.10.32	57375	119.46.151.200	53
medium	10/23 23:18:23	spyware	Suspicious DNS Query (generic:lgolapapdv.biz)	172.18.10.32	58397	119.46.151.200	53
medium	10/23 23:18:13	spyware	Suspicious DNS Query (generic:wnzgge.com)	172.18.10.32	56848	119.46.151.200	53
medium	10/23 23:06:34	spyware	Suspicious DNS Query (generic:ujpedirewb.cc)	172.18.10.31	59303	203.155.33.2	53
medium	10/23 23:06:34	spyware	Suspicious DNS Query (generic:minvpoczdk.cn)	172.18.10.31	58383	203.155.33.2	53
medium	10/23 23:06:34	spyware	Suspicious DNS Query (generic:wnopsx.org)	172.18.10.31	58407	203.155.33.2	53
medium	10/23 23:06:34	spyware	Suspicious DNS Query (generic:ebmok.info)	172.18.10.31	57620	203.155.33.2	53

รูปที่ 1.1 ตัวอย่าง Log Anti-spyware ของอุปกรณ์ Paloalto

โครงงานชิ้นนี้จัดทำขึ้นเพื่อขยายความของ Alert ที่เกิดขึ้นและหาเครื่องที่ติด Malwares จริงๆ โดยนำหลักการของ Honeypot มาทำเป็น Reverse Honeypot และนำ Access Log ที่เกิดขึ้นมาตรวจจับเครื่องที่ติด Malwares และเพิ่มความแม่นยำการวิเคราะห์เหตุการณ์ได้ดีขึ้น

1.2 แนวทางการแก้ปัญหา

ปัจจุบันระบบที่ตรวจสอบ Anti-Malwares ของ Next-Generation Firewall ส่วนใหญ่จะตรวจสอบจาก DNS Query ของเครื่องต้นทาง หาก Query Domain ที่เป็น Blacklist Domain จะสามารถเลือก Action บางอย่างที่ต้องการได้เช่น Allow, Block หรือ แปรงให้เป็นหมายเลขไอพีที่ต้องการ (Sinkhole) และพฤติกรรมของ Malwares ส่วนใหญ่เมื่อติดต่อกลับไปยัง C&C Server จะใช้เป็น Protocol HTTP และ HTTPS เพื่อหลบเลี่ยงการตรวจจับและ Firewall ส่วนใหญ่จะเปิดการใช้งานสำหรับ 2 Protocol นี้ จึงต้องมี Server ที่ให้บริการเรื่อง Web เพื่อเก็บ Log Access และให้ Next-Generation Firewall ตอบไอพีของ Blacklist Domain ให้เป็นหมายเลขไอพีของ Web Server ดังกล่าวเพื่อนำ Log Access ดังกล่าวมาทำ Alert และ Report ต่อไป

1.3 วัตถุประสงค์

1.3.1 เพื่อหาเครื่องที่ติด Malwares ได้ถูกต้อง

1.3.2 เพื่อเพิ่มความแม่นยำในการวิเคราะห์และตรวจจับภัยคุกคามได้แม่นยำมากขึ้น

1.3.3 เพื่อตอบสนองต่อเหตุการณ์เครื่องที่ติด Malware ได้รวดเร็วยิ่งขึ้น

1.3.4 เพื่อเพิ่มประสิทธิภาพการตรวจจับภัยคุกคามภายในหน่วยงาน

1.4 ภาพรวมของระบบที่จัดทำ

1.4.1 Paloalto เป็นอุปกรณ์ Next-Generation Firewall ถูกวางไว้หลัง Router และมีการจัดแบ่งระบบเครือข่ายเป็นโซนดังนี้ Internet zone, DMZ zone และ Core Switch zone เพื่อให้เกิดความสะดวกในการควบคุมและจัดการ

1.4.2 NginX เป็นอุปกรณ์ Reverse Proxy ซึ่งมีความสามารถในการแยก Host ที่เรียกยัง Web Server เพื่อแยกชนิดของมัลแวร์ และ Log มีความละเอียด

1.4.3 Splunk เป็นอุปกรณ์ Security Information and Event Management (SIEM) ไว้สำหรับเก็บ Log จาก NginX เพื่อนำมาวิเคราะห์ แจ้งเตือนและทำ Report

1.5 ขอบเขตของการทำงานระบบ

1.5.1 ทำ Reverse Proxy เพื่อเก็บ Log Access จากเครื่องที่ติด Malwares

1.5.2 นำ Log Access ที่ได้ส่งไปที่ SIEM ไว้สำหรับ Query ข้อมูลและ Report

1.5.3 ตรวจสอบเครื่องคอมพิวเตอร์ลูกข่ายที่มีใน Report

1.6 โครงสร้างของสารนิพนธ์

สารนิพนธ์นี้แบ่งเนื้อหาออกเป็น 5 บท สรุปได้ดังต่อไปนี้

1.6.1 บทที่ 1 เป็นการกล่าวถึงที่มาและปัญหาของการตรวจจับมัลแวร์ที่ Next-Generation Firewall ภายในระบบเครือข่ายของหน่วยงาน

1.6.2 บทที่ 2 เป็นการกล่าวถึงพื้นฐานและทฤษฎีที่เกี่ยวข้องของของระบบ

1.6.3 บทที่ 3 เป็นการกล่าวถึงภาพรวมและโครงสร้างของระบบ รวมถึงรายละเอียดต่างขององค์ประกอบอาทิเช่น การรับส่งข้อมูลแต่ละจุด รวมถึงการทำงานของแต่ละอุปกรณ์

1.6.4 บทที่ 4 เป็นผลการดำเนินงานตามขอบเขตที่ได้กำหนดไว้ โดยจะมีวิธีการทดลองและผลการทดลองในแต่ละอุปกรณ์ที่ได้ออกแบบไว้

1.6.5 บทที่ 5 เป็นการสรุปผลการดำเนินงานสารนิพนธ์ ปัญหาและอุปสรรค และคำแนะนำเพิ่มเติมเพื่อเป็นแนวทางในการนำไปประยุกต์ใช้

บทที่ 2

พื้นฐานและทฤษฎีที่เกี่ยวข้อง

2.1 มัลแวร์

มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software เป็นโปรแกรมที่มีประสงค์ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์นั้นสามารถแบ่งออกได้หลากหลายประเภทเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าจโทรจันทร์ (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Browser ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์ ซึ่งหลังจากที่มัลแวร์ติดตั้งบนเครื่องคอมพิวเตอร์สำเร็จ มัลแวร์ติดต่อกลับไปยัง Server ของผู้ประสงค์ร้ายหรือที่เรียกกันว่า C&C Server เพื่อที่จะรอรับคำสั่งอื่นจากผู้ประสงค์ร้ายหรือส่งข้อมูลบนเครื่องคอมพิวเตอร์ออกไปภายนอกเป็นต้น

2.1.1 ประเภทหลักๆของมัลแวร์

1) Trojan Horse เป็นมัลแวร์ที่ทำตัวเหมือนโปรแกรมปกติ เช่น โปรแกรม Download VDO จาก Youtube, โปรแกรม Crack Software ต่างๆ, โปรแกรม key gen ที่สร้าง Serial Number ไว้สำหรับ Register โปรแกรมลิขสิทธิ์ต่างๆ เป็นต้น ซึ่งโปรแกรมเหล่านี้จะหลอกให้ผู้ใช้งานดาวน์โหลดมาใช้งาน แต่หลังจากที่ติดตั้งแล้วจะเปิดช่องทางให้ผู้ประสงค์ร้ายเข้าควมคุมหรือขโมยข้อมูลจากเครื่องที่ติดตั้งได้
2) Worm คุณสมบัติพิเศษของเวิร์ม คือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ โดยอาศัยอีเมลล์หรือช่องโหว่ของระบบปฏิบัติการผ่านทางเครือข่าย เวิร์มบางประเภทสามารถแพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยเหลือจากผู้ใช้เลย หรือบางตัวก็อาจแพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรม สิ่งที่เวิร์มมันทำคือมักจะสร้างความเสียหายให้กับระบบเครือข่าย

3) Virus คือมัลแวร์ประเภทหนึ่งที่สามารถคัดลอกตัวเองกระจายไปยังเครื่องอื่นๆ โดยผ่าน ไฟล์ประเภทต่างๆ เช่น Script file, Document File ,สร้าง Autorun ให้ Flash Drive ที่ต่อเข้ากับคอมพิวเตอร์ เป็นต้น เมื่อติดไวรัสแล้วจะส่งผลหลายอย่างเช่น อาจจะถูกขโมยข้อมูล ทำเครื่องที่โดนไวรัสช้า หรือ หยุดทำงานตลอดเวลา
4) Spyware จะทำการเก็บข้อมูลการใช้งานต่างๆ ของเครื่องที่ถูกติดตั้ง แล้วส่งไปยังผู้ประสงค์ร้าย ตัวอย่างเช่นโปรแกรม Keylogger เป็นมัลแวร์ที่เก็บทุกแป้นที่พิมพ์ที่ผู้ใช้พิมพ์ (ส่วนใหญ่ Capture หน้าจอไปพร้อมๆกันด้วย) โดยที่ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ ต้องอาศัยการหลอกคนใช้ให้ดาวโหลดเอาไปใส่เครื่องเองหรืออาศัยช่องโหว่ของ web browser ในการติดตั้งตัวเองลงในเครื่อง

2.1.2 ผลกระทบเมื่อถูกติดตั้งมัลแวร์ในปัจจุบัน

1) หากถูกควบคุมเครื่องคอมพิวเตอร์ด้วย Trojan Horse ผู้ประสงค์ร้ายอาจใช้ไปโจมตีเครื่องอื่นต่อเช่น Dos, DDos เป็นต้น โดยที่เครื่องที่ถูกติดตั้ง Trojan Horse ประเภทนี้จะถูกเรียกว่า Bot หรือ Zombie
2) ใช้ทรัพย์พยากรในการขุด Bit Coin ส่งผลให้เครื่องคอมพิวเตอร์ทำงานช้า
3) ถูกเข้ารหัสไฟล์หรือที่เรียกกันว่า Ransomware ซึ่งหากผู้ประสงค์ร้ายเข้ามาที่เครื่องได้ไม่ว่าจะช่องทางไหน หากสามารถควบคุมเครื่องดังกล่าวได้ จะทำการเข้ารหัสไฟล์แล้วส่ง Key ในการถอดรหัสไฟล์กลับไปยัง C&C Server
4) ถูกขโมยข้อมูลในเครื่อง ข้อมูล User password และอื่นๆ
5) หากถูกติดตั้ง Worm จะส่งผลให้เครื่องดังกล่าวพยายามติดตั้ง Worm ไปยังเครื่องข้างเคียง ซึ่งส่งผลให้ระบบเครือข่ายภายในมีปัญหาได้

2.1.3 ข้อแนะนำในการป้องกันการติดมัลแวร์

1) อัพเดทคอมพิวเตอร์และซอฟแวร์ในเครื่องสม่ำเสมอ
2) ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์

3) ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดรฟ์ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน

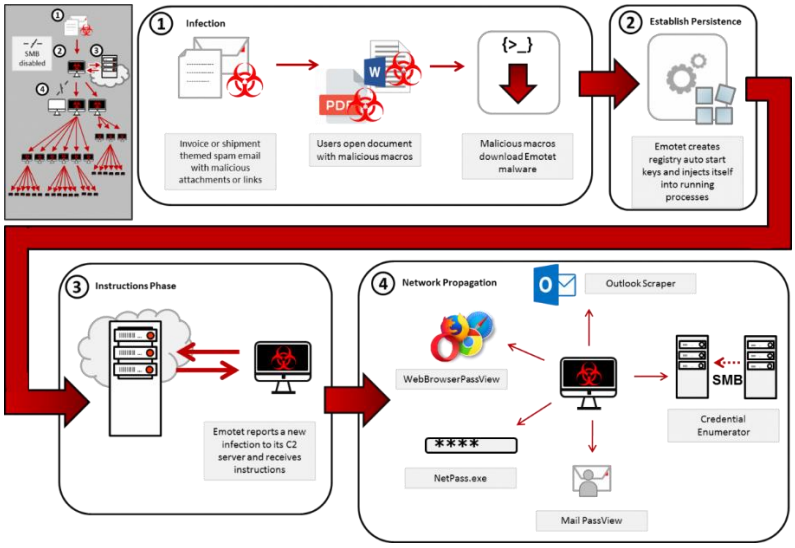
4) ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ

5) ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่

6) หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใดๆที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

2.1.4 ตัวอย่างมัลแวร์ชื่อ Trojan.Emotet

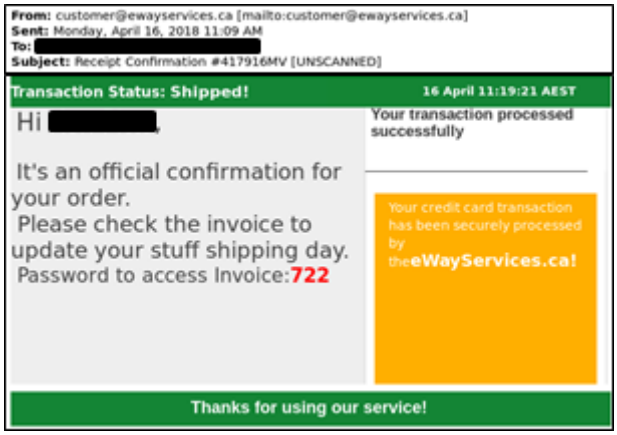
Emotet เป็นมัลแวร์ประเภท Trojan ที่มีเป้าหมายไปที่ธนาคาร ซึ่งทำหน้าที่ Download Trojan ตัวอื่นๆมาติดตั้งที่เครื่องเหยื่อเพิ่มเติม ซึ่ง Emotet นั้นสร้างความเสียหายมากมาย ขั้นตอนการทำงานแต่ละขั้นตอนดังรูปที่ 2.1



รูปที่ 2.1 กระบวนการต่างๆของ Trojan.Emotet

Emotet นั้นใช้วิธีการแพร่กระจายในระดับ Public Internet ผ่าน Spam mail โดยที่แอบชื่อผู้ส่งโดยใช้ชื่อแบรนด์เนมที่คุ้นเคย ซึ่งมี Case ตัวอย่างโดยที่เลียนแบบใบเสร็จของ

Paypal และแจ้งเตือนการจัดส่งใบแจ้งหนี้ โดยแนบไฟล์มาในรูปแบบของ Microsoft Word หรือ PDF ซึ่งหากเปิดไฟล์ดังกล่าว Emotet จะเริ่มแพร่กระจายใน Local Network ดังรูปที่ 2.2



รูปที่ 2.2 ตัวอย่าง Spam mail ที่ใช้สำหรับแพร่กระจาย Trojan.Emotet

สำหรับวิธีการแพร่กระจายใน Local Network ที่หลังจาก Emotet เริ่มทำงานมีทั้งหมด 5 กระบวนการ คือ NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, และ credential enumerator

1. NetPass.exe เป็นโปรแกรมสำหรับกู้ password ผ่าน Local Network ของผู้ใช้งานที่ logon อยู่
2. Outlook Scraper เป็นโปรแกรมสำหรับรวบรวมรายชื่อ Email Address ใน Outlook ไว้สำหรับส่ง Email Phishing ต่อไป
3. WebBrowserPassView เป็นโปรแกรมสำหรับกู้รหัสผ่านที่อยู่ใน Browser ต่างๆ
4. Mail PassView เป็นโปรแกรมสำหรับแสดง Email Client และรหัสผ่านเช่น Microsoft Outlook Windows Mail, Mozila Thunderbird เป็นต้น
5. Credential Enumerator เป็นกระบวนการทดสอบเข้าสู่เครื่องอื่นโดยผ่าน SMB หรือไฟล์แชร์ หากเข้าไม่ได้จะทดสอบ Brute Force เพื่อหา Administrator Account

2.2 DNS

DNS (Domain name system) จะทำหน้าที่แปลงข้อมูลจากชื่อให้กลายเป็นหมายเลข IP (IPv4 or IPv6) เพราะหากให้จำหมายเลข IP เข้าเวปไซท์ใดเว็ปไซท์หนึ่งคงเป็นเรื่องยาก แต่หากจำจากชื่อก็เป็นเรื่องที่ง่าย ทำให้ DNS เกิดขึ้นมาเพื่อตอบโจทย์การเข้าถึงเว็ปไซท์ต่างๆ

2.2.1 หน้าที่ของ DNS แบ่งได้ดังต่อไปนี้

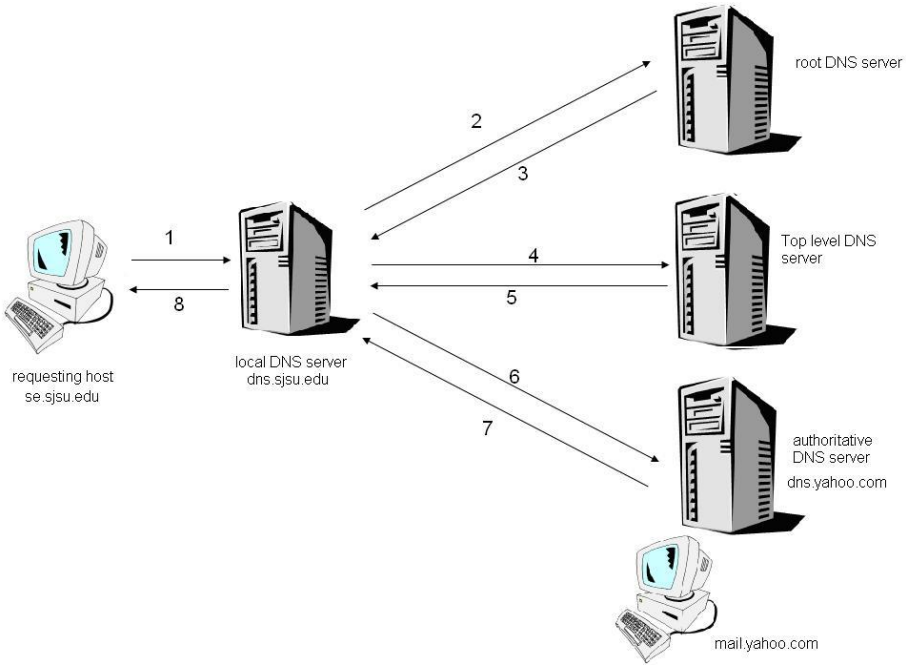
1) Hostname to IP - ทำหน้าที่ในการแปลงค่าระหว่างชื่อกับหมายเลข IP เช่น www.mut.ac.th แปลงเป็น 203.188.27.26 เป็นต้น
2) Host aliasing หรือ CNAME(Cannonical Name) - cname เป็นการ map ชื่อ subdomain ไปยัง Hostname ที่คุณต้องการอีกที่หนึ่ง เช่น mail.mut.ac.th ได้ทำการ map แบบ cname ไปยัง webmail.mut.ac.th เมื่อพิมพ์ mail.mut.ac.th วิ่งมาที่ Server webmail.mut.ac.th และแสดงผลหน้าเว็บทันที ด้วยวิธีนี้จะช่วยให้สามารถ map ชื่อ subdomain ไปยัง hostname ปลายทางใดๆ ก็ได้ โดยการ map แบบ cname ถือเป็นวิธีหนึ่งที่ได้รับความนิยม เนื่องจากเป็นการ map ในลักษณะ Hostname เช่น Hostname ปลายทาง คือ webmail.mut.ac.th เมื่อ Hostname ปลายทางมีการเปลี่ยน IP ของ Server Hostname: webmail.mut.ac.th เป็นค่า IP อื่นๆ web ต้นทางก็ไม่ต้องกังวล เพราะยังไง cname ก็มีค่าเท่ากับ webmail.mut.ac.th อยู่แล้ว โดยไม่สนใจว่าจะมีการเปลี่ยน IP เป็นอะไร
3) Mail server aliasing - ทำหน้าที่บอกว่า Mail Server ของ Domain ดังกล่าวมี IP อะไร

2.2.2 ในระบบ DNS จะมีการแบ่งออกเป็น 3 ลำดับชั้นดังนี้

1) Root DNS Servers - ปัจจุบันมีอยู่ 13 เครื่อง คือ a.rootserver.net ถึง m.rootserver.net
2) Top Level Domain (TLD) - เป็นเครื่องที่ใช้เก็บข้อมูล Domain ที่ลงท้ายตามชื่อของแต่ละโดเมนเช่น .com, .net, .org, .th เป็นต้น
3) Authoritative - เป็น Domain name server ที่มีการดูแลโดยองค์กรต่างๆ เช่น google.com, facebook.com, amazon.com เป็นต้น

2.2.3 การ Query DNS มี 2 วิธี

1) Iterated Query โดยมีวิธีการทำงานดังรูปที่ 2.3



รูปที่ 2.3 Iterated Query

1.1) Client ถามไปยัง local DNS ว่า mail.yahoo.com มี ip อะไร

1.2) local DNS จะถามต่อไปยัง root เพื่อสอบถาม ip ของ mail.yahoo.com

1.3) root จะตอบ ip ของ Top level DNS ของ .com มาให้

1.4) local DNS จะถามต่อไปยัง Top level DNS ของ .com เพื่อสอบถาม ip ของ mail.yahoo.com

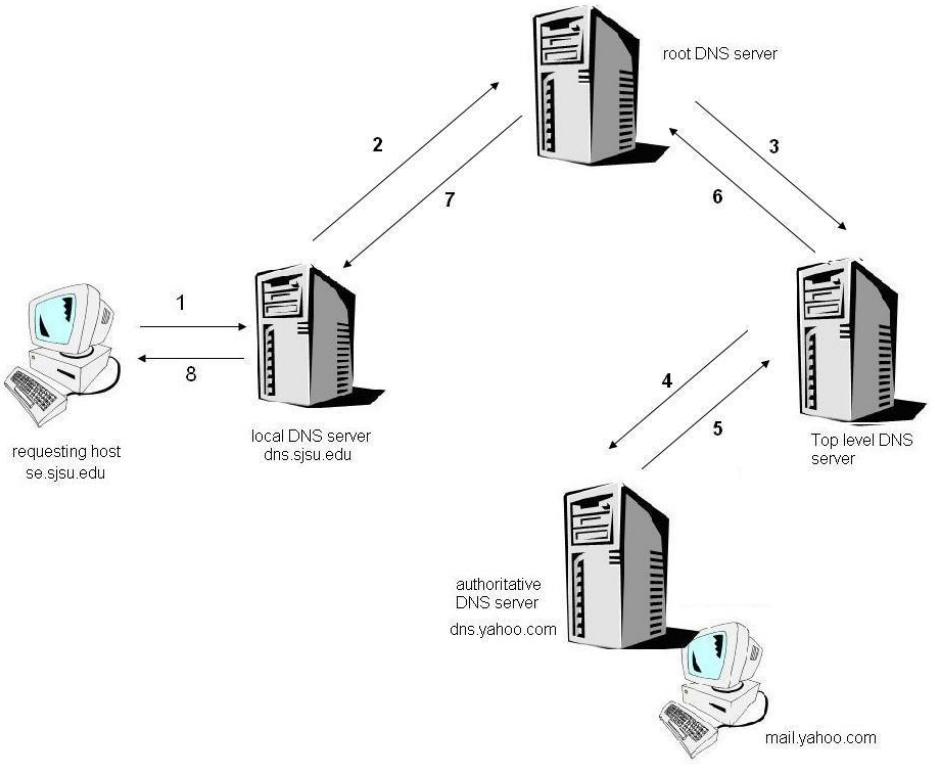
1.5) Top level DNS ของ .com จะตอบ ip ของ Authoritative dns server ของ yahoo.com มาให้

1.6) local DNS จะถามต่อไปยัง Authoritative dns server ของ yahoo.com เพื่อสอบถาม ip ของ mail.yahoo.com

1.7) Authoritative dns server ของ yahoo.com จะตอบ ip ของ mail yahoo.com มาให้

1.8) local DNS จะตอบ ip ของ **www.yahoo.com** กลับไปที่ Client

2) Recursive query โดยมีวิธีการทำงานดังรูปที่ 2.4



รูปที่ 2.4 Recursive query

2.1) Client ถามไปยัง local DNS ว่า mail.yahoo.com มี ip อะไร

2.2) local DNS จะถามต่อไปยัง root เพื่อสอบถาม ip ของ mail.yahoo.com

2.3) root จะถามต่อไปยัง Top level DNS ของ .com เพื่อสอบถาม ip ของ mail.yahoo.com

2.4) Top level DNS ของ .com จะถามต่อไปยัง Authoritative dns server ของ yahoo.com เพื่อสอบถาม ip ของ mail.yahoo.com

2.5) Authoritative dns server ของ yahoo.com จะตอบ ip ของ mail yahoo.com มาให้ Top level DNS ของ .com

2.6) Top level DNS ของ .com จะตอบ ip ของ mail yahoo.com มาให้ root

2.7) root จะตอบ ip ของ mail yahoo.com มาให้ local DNS

2.8) local DNS จะตอบ ip ของ mail yahoo.com มาให้ Client

2.3 Next-Generation Firewall

Next Generation Firewall คือ Firewall ที่มีความสามารถในการมองเห็น application ในระดับ Layer 7 (Application Layers) ของ OSI Layer และมีความสามารถอื่น ๆ อาจมีความสามารถของ IPS ในการตรวจจับการโจมตีแบบต่าง ๆ ทั้งในแบบ ระบบการตรวจสอบโดยการใช้ signature, การตรวจสอบพฤติกรรมที่ผิดปกติ (Behavior) เป็นต้น ซึ่งความสามารถพื้นฐานที่อุปกรณ์ Next Generation Firewall นั้นจะต้องทำได้ อาทิเช่น

1) จะต้องสามารถทำการระบุและกรอง Application ได้ ข้อนี้ถือได้ว่าเป็นหัวใจหลักของ Next Generation Firewall โดยสามารถกรอง Traffic โดยระบุเป็น Application แทนที่จะสามารถเลือกกรองในรูปแบบของ Port เหมือน Traditonal Stateful Firewall ทั่วไป
2) จะต้องทำงานตามมาตรฐานของอุปกรณ์ Firewall มาตรฐานได้ เช่น เป็น Stateful Protocol Inspection สามารถทำ Routing ทำ Network Address Translation (NAT) และ Port Address Translation (PAT) สามารถทำ Virtual Private Network(VPN) ได้
3) สามารถป้องกันการโจมตี โดยจะต้องมีความฉลาดและสามารถทำงานในลักษณะ deep packet inspection ได้ อีกทั้งยังอาจจะมีความสามารถของระบบ Intrusion Prevention System ด้วย
4) สามารถทำ SSL Inspection ได้เพื่อป้องกัน Application ที่อาศัยช่องโหว่ของการ Encrypt โดยตัวอุปกรณ์จะต้องสามารถที่จะ Decrypt SSL Traffic และทำการตรวจสอบ Application และตรวจสอบ Policy ต่าง ๆ จากนั้นทำการ Re-encrypt Traffic นั้นเป็น SSL อีกครั้งก่อนส่งให้กับปลายทาง
5) สามารถทำงานร่วมกับ Directory เช่น ตรวจสอบ User จาก Directory ตัวอย่างเช่น Microsoft Active Directory เพื่อกำหนด Policy โดยอาศัย User และ Group ภายใน Directory แทนที่จะกำหนดเป็น Source Address หรือ Destination Address ในการให้ Policy เป็นต้น
6) สามารถทำ Malware filtering โดยสามารถตรวจสอบและป้องกันโปรแกรมจำพวก Phishing , Virus และ Malware Application ต่าง

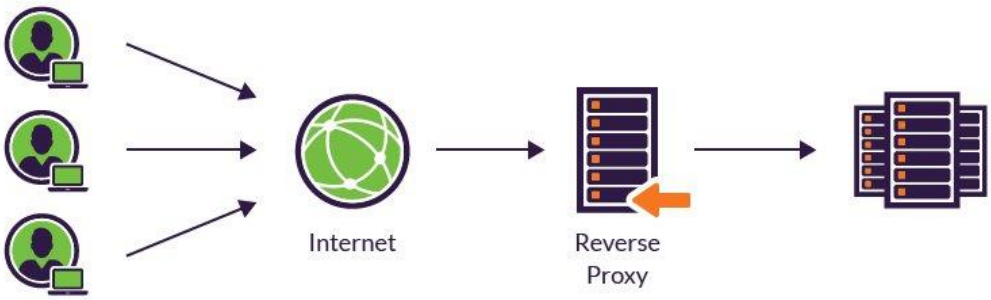
2.3.1 Malware Filtering

หลักการทำงานของ Malware Filtering นั้นจะไม่เหมือนกับ Anti-Virus ทั่วไปที่จะต้องไปติดตั้งโปรแกรมที่เครื่องคอมพิวเตอร์ และตรวจสอบจาก Hash ไฟล์ต่างๆที่อยู่ในเครื่องคอมพิวเตอร์เครื่องนั้นเทียบกับข้อมูลจาก Hash ไฟล์ที่เป็นไฟล์ Malware ต่างๆ โดยที่ Next Generation Firewall จะตรวจสอบจาก Domain ที่ถูก Query ซึ่ง Traffic ดังกล่าวจากต้องผ่านอุปกรณ์ Next Generation Firewall และหาก Domain ดังกล่าวอยู่ในรายการของ Domain อันตรายหรือ C&C Server จะสามารถยับยั้งการ Query ดังกล่าวได้ โดยการยับยั้งนั้นมีด้วยกัน 2 วิธี

1) Block ซึ่งการ Block นั้นอาจทำให้ Malware ดังกล่าวพยายามที่จะ Query เป็นจำนวนมาก ซึ่งส่งผลต่อการทำงานของ Next Generation Firewall ให้ทำงานหนักขึ้นได้
2) Sinkhole คือการที่เปลี่ยนแปลง IP ของ Domain ดังกล่าวเป็น IP ที่ตั้งค่าไว้ สามารถช่วยลด Traffic จากการ Query DNS ของ Malware ได้

2.4 Reverse Proxy

ทำหน้าที่เป็นสื่อกลางระว่าง User กับ Web Server โดยที่ Reverse Proxy จะรับ HTTP Request มาจาก User และส่งต่อไปยัง Web Server ปลายทาง เพื่อเก็บ Information ของ Website ซึ่งเป็นการลดภาระการทำงานของ Web Server เพื่อไม่ให้ Web Server ทำงานหนักเกินไป ดังรูปที่ 2.5



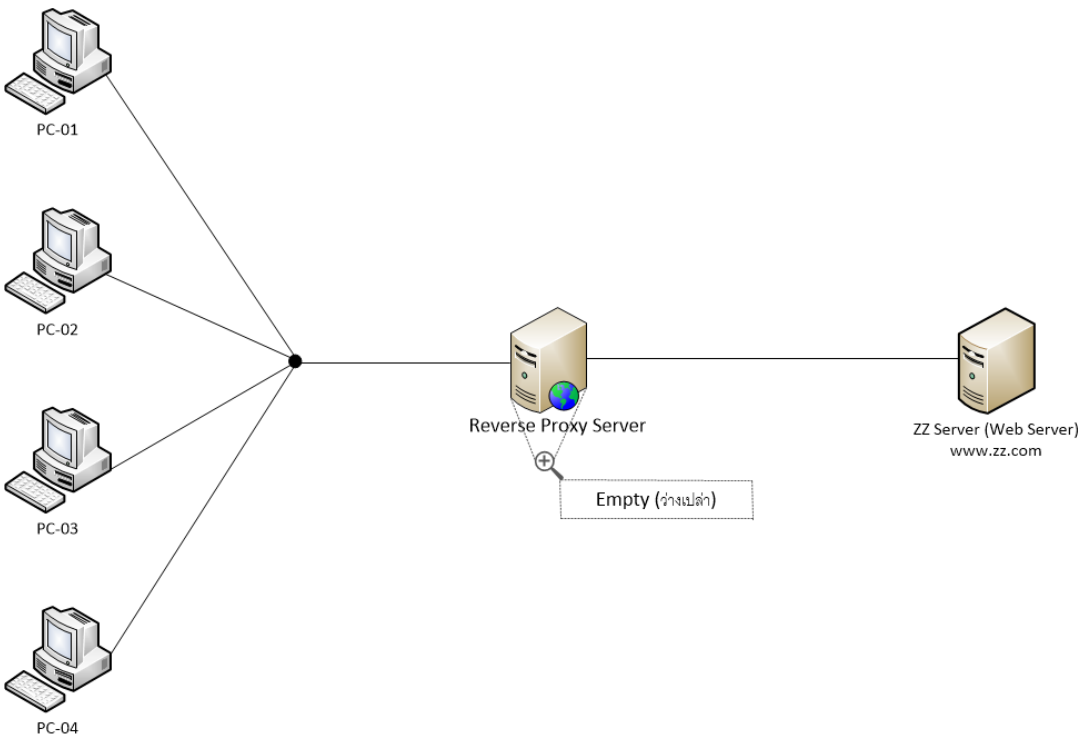
รูปที่ 2.5 แสดงการทำงานของ Reverse Proxy

2.4.1 หลักการทำงานของ Reverse Proxy

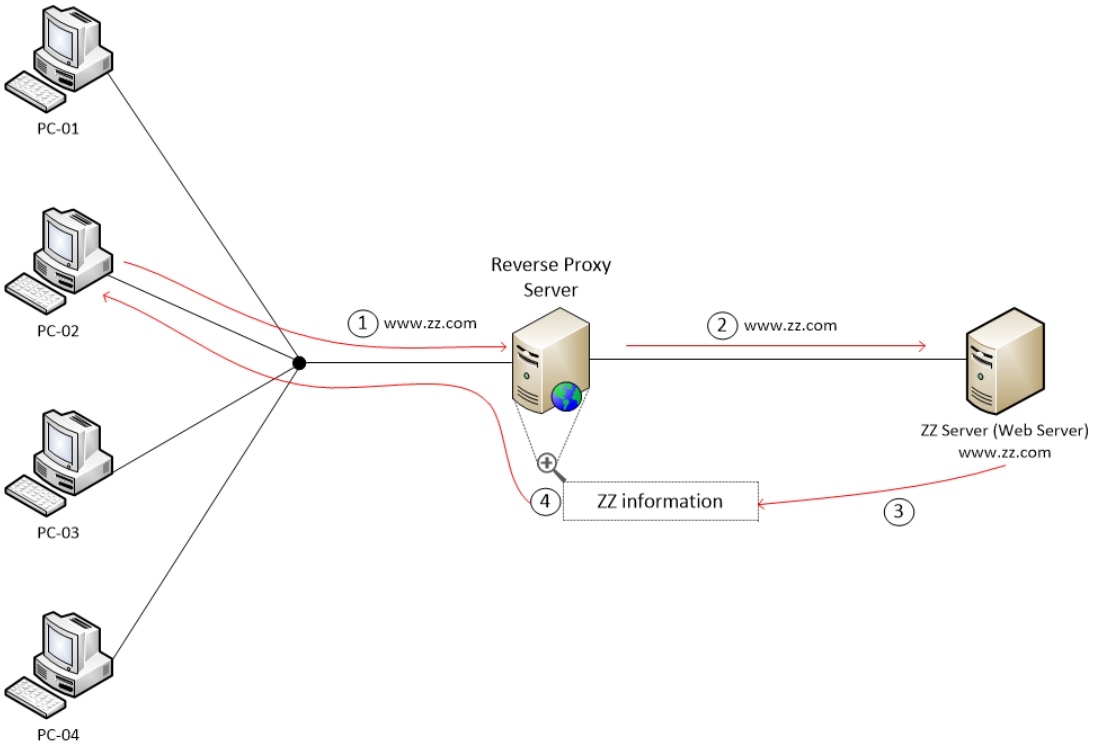
1) User เข้าใช้งานเว็บไซต์โดยต้องเรียกผ่านชื่อ Domain Name เท่านั้นหลังจาก Query DNS แล้ว IP ที่ได้มาจะต้องเป็น IP ของ Reverse Proxy
2) เมื่อ Reverse Proxy ได้รับ HTTP Request แล้ว Reverse Proxy จะตรวจสอบ Header ใน HTTP ว่า Domain Name ของเว็บไซต์ที่เรียกมาคืออะไร หากมี Domain Name ตรงกับที่ตั้งค่าเอาไว้ Reverse Proxy จะส่ง HTTP Request ตามที่ตั้งค่าเอาไว้ โดยที่จะต้องจับคู่กับระว่าง Domain กับ IP Server ปลายทาง
3) ซึ่ง Reverse Proxy 1 ตัวสามารถลองรับ Traffic ได้หลากหลาย Domain

2.4.2 ตัวอย่างการทำงานของ Reverse Proxy

เครื่อง PC-01 ถึง PC-04 ยังไม่มีการเข้าใช้งาน www.zz.com ดังรูปที่ 2.6



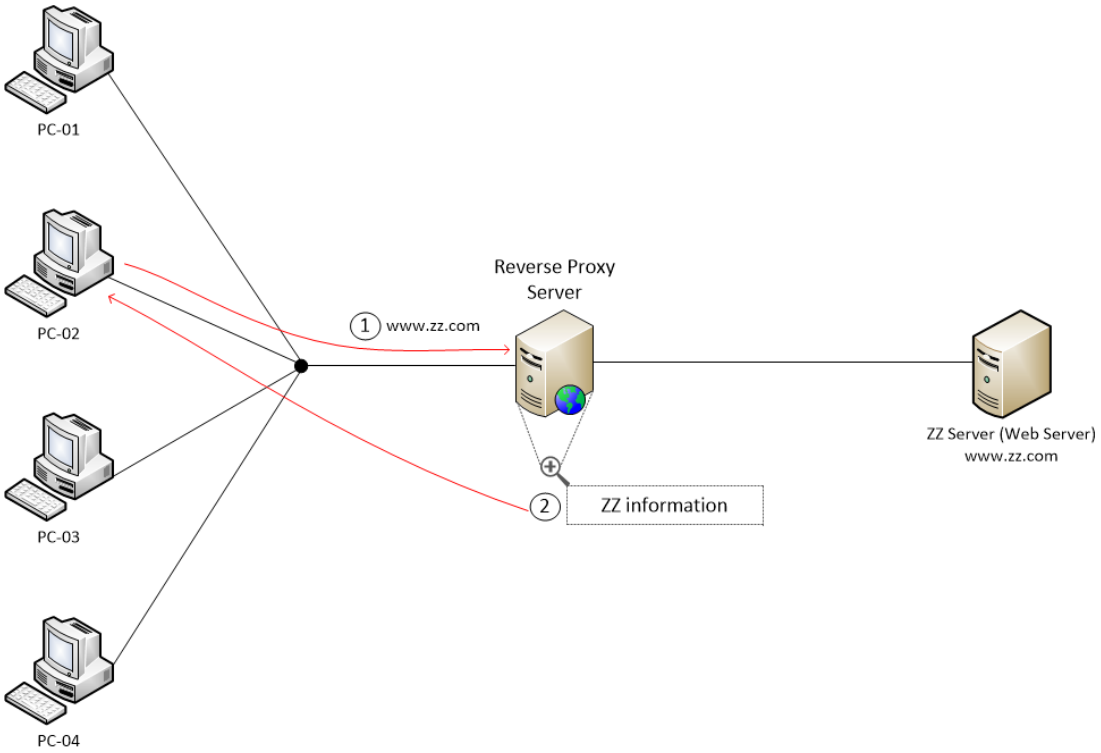
รูปที่ 2.6 ตัวอย่างการทำงานของ Reverse Proxy (1)



รูปที่ 2.7 ตัวอย่างการทำงานของ Reverse Proxy (2)

จากรูปที่ 2.7

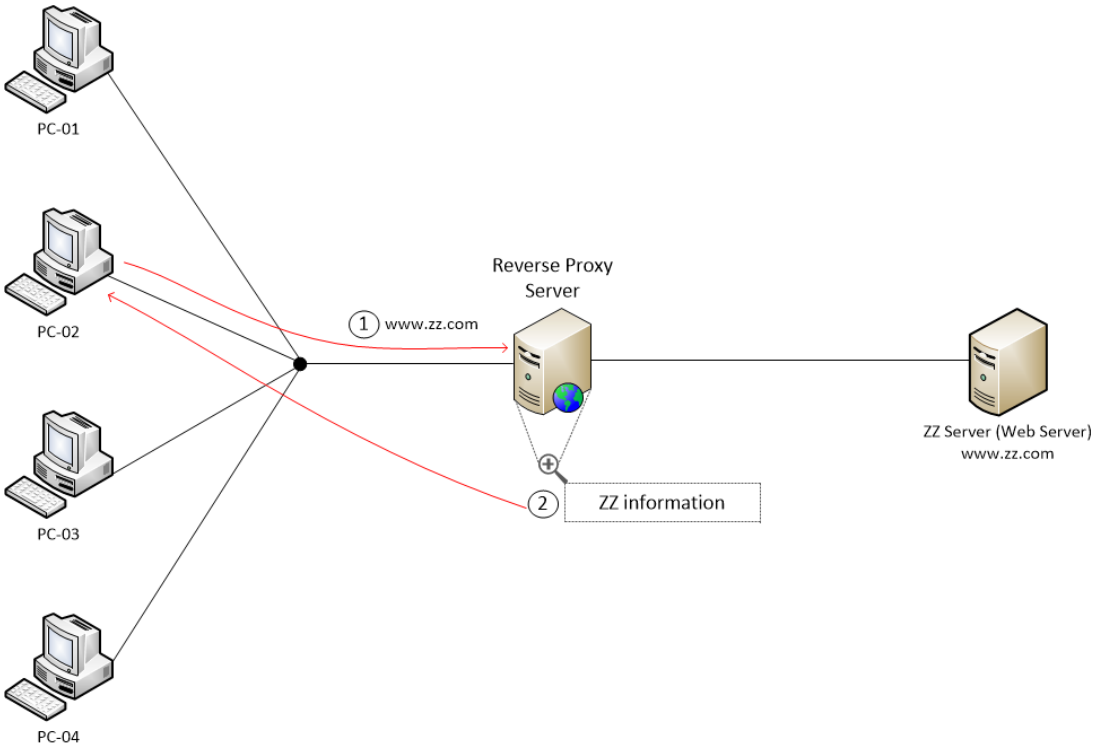
1) เครื่อง PC-02 ต้องการเข้าใช้ www.zz.com
2) Reverse Proxy Server ทำการส่ง Request ไปหา ZZ Server
3) ZZ Server ทำการ Response ตัว Information มายัง Proxy Server
4) Reverse Proxy Server ทำการ Response ตัว Information ไปให้ PC-02



รูปที่ 2.8 ตัวอย่างการทำงานของ Reverse Proxy (3)

จากรูปที่ 2.8

1) เครื่อง PC-02 ต้องการเข้าใช้ www.zz.com
2) Information ของ ZZ Server มีอยู่ใน Cache แล้ว ดังนั้นจึงทำการ Response ตัว Information ไปยัง PC-02 ได้เลย



รูปที่ 2.9 ตัวอย่างการทำงานของ Reverse Proxy (4)

จากรูปที่ 2.8

1) เครื่อง PC-01 ต้องการเข้าใช้ www.zz.com
2) 2. Information ของ ZZ Server มีอยู่ใน Cache แล้ว ดังนั้นจึงทำการ Response ตัว Information ไปยัง PC-01 ได้เลย

2.4.3 ผลประโยชน์จากการใช้งาน Reverse Proxy

1) สามารถทำ SSL ให้กับ Web Server บน Reverse Proxy ได้
2) สามารถให้ Reverse Proxy Request ไป Port อื่นแทนได้ที่ไม่ใช่ 80,443
3) สามารถทำเป็น Web Appicatione Firewall (WAF) ได้
4) Reverse 1 เครื่อง ลองรับ Web Server ได้มาก
5) สามารถเก็บ Custom Log ให้มีความละเอียดมากขึ้น
6) สามารถเก็บไข Header ได้ก่อนที่จะถูกส่งไปยัง Server ปลายทาง

2.5 Security Information and Event Management (SIEM)

SIEM คือระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่าย เพื่อนำข้อมูลเหล่านั้นไปใช้ในการโต้ตอบการโจมตีที่เกิดขึ้น, การตรวจสอบการกระทำผิด และการทำ Compliance ภายในองค์กรนั่นเอง โดยพื้นฐานแล้ว ข้อมูลที่จะนำมาทำการวิเคราะห์นี้จะเป็นข้อมูล Log จากอุปกรณ์รักษาความปลอดภัยเครือข่าย, อุปกรณ์เครือข่าย, ระบบงานต่างๆ และ Application จากนั้นนำ Log ที่ได้หาความสัมพันธ์ เพื่อค้นหาพฤติกรรมการโจมตีระบบเครือข่ายที่กำลังเกิดขึ้น และทำการแจ้งเตือนผู้ดูแลระบบแบบ Real-time ปัจจุบันความก้าวหน้าทางเทคโนโลยีและราคาที่ถูกลงของฮาร์ดแวร์ ทำให้ผู้ผลิตระบบประมวลผลข้อมูล log เพิ่มความสามารถในผลิตภัณฑ์ของตนเองและเรียกระบบเหล่านี้เป็น SIEM แทบทั้งสิ้น หากจะให้นิยามระบบดังกล่าวอย่างน้อยต้องมีความสามารถดังต่อไปนี้

- **Data Collection** คือความสามารถในการรวบรวมข้อมูล log จาก Server และอุปกรณ์ที่สามารถส่ง Log ได้ ทั้งแบบการส่งข้อมูลมายัง SIEM โดยตรงด้วย Syslog หรือติดตั้งตัวจัดเก็บข้อมูล (Collector Sensor) Server และอุปกรณ์ที่สามารถส่ง Log ได้ คุณสมบัติข้อนี้มีความสำคัญในแง่ที่ว่า Server และอุปกรณ์ที่สามารถส่ง Log ใช้ระบบปฏิบัติการที่แตกต่างกัน จัดเก็บข้อมูล log ในรูปแบบที่แตกต่างกัน ซึ่งผู้ผลิต SIEM แต่ละราย จะระบุรายการของอุปกรณ์และระบบปฏิบัติการ
- **Aggregation** คือความสามารถในการรวบรวมข้อมูลจากข้อมูล log ที่รับมาจากอุปกรณ์ต่าง ๆ ซึ่งมีรูปแบบข้อมูลที่แตกต่างกัน นำมาจัดเก็บให้อยู่ในรูปแบบเดียวกัน เพื่อประโยชน์ในวิเคราะห์และแสดงผล โดยทั่วไปอุปกรณ์กำเนิดข้อมูล log เช่น Router Firewall IPS รวมทั้ง Database และ Web Server ต่างก็มีรูปแบบข้อมูล log ของตนเอง SIEM จะต้องสามารถนำข้อมูลมาจัดเก็บในรูปแบบมาตรฐานและลดความซ้ำซ้อน (Normalization) ของข้อมูลที่รับมาจัดเก็บไว้ในระบบ SIEM โดยต้องคงความหมายของข้อมูลเดิมไว้ และจัดเก็บให้ง่ายต่อการสืบค้นและการประมวลผล เนื่องจากข้อมูล log มีปริมาณมากและซ้ำซ้อนเป็นธรรมชาติ พื้นที่ในการจัดเก็บและประสิทธิภาพในการเข้าถึงข้อมูล log จึงขึ้นกับความสารมารถในการรวบรวมข้อมูลและการทำ

- **Correlation** คือความสามารถในการหาความสัมพันธ์ของข้อมูล ตามเงื่อนไขที่กำหนดไว้ ตัวอย่างเช่น “มี IP ใดบ้างที่เชื่อมต่อเข้ามายัง IP ภายในองค์กรด้วย Port ที่สูงกว่า 1024 และถูก Firewall หรือ IPS ตัดการเชื่อมต่อมากกว่า 1,000 เหตุการณ์ต่อ 10 นาที ภายใน 24 ชั่วโมง” หรือ “มี IP ภายในองค์ใดบ้างที่เชื่อมต่อออกไปยัง IP ภายนอกโดยมีพอร์ตต้นทางเป็น 56444 และหมายเลขพอร์ตปลายทางเป็น 16464 หรือ 16465” หรือ “มี IP ใดบ้างที่เชื่อมต่อเข้ามายังเว็บเซิฟเวอร์ขององค์กรด้วยหมายเลขพอร์ตปลายทางที่ไม่ใช่พอร์ต 80 เป็นจำนวนมากกว่า 6000 เหตุการณ์ต่อ 10 นาที” เป็นต้น
- **Alerting** คือความสามารถในการแจ้งเตือนไปยังผู้ดูแลระบบ เมื่อตรวจพบข้อมูล log ที่สอดคล้องกับเงื่อนไขที่ตั้งไว้หรือเมื่อมีการตรวจพบผลของการทำ Correlation ตามเงื่อนไขที่กำหนด ซึ่งระบบการแจ้งเตือนควรจะต้องส่งผ่านช่องทาง อีเมลได้เป็นอย่างน้อย เพื่อให้ผู้ดูแลระบบหรือผ้เกี่ยวข้องรับมือกับเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที
- **Dashboards** นำเสนอกระดานแสดงสถานะข้อมูลระบบ เพื่อให้ผู้ดูแลระบบบริหารจัดการข้อมูลได้สะดวก เนื่องจาก SIEM นั้นเป็นมีข้อมูลข่าวสารที่สำคัญหลากหลายซึ่งไม่สะดวกและไม่ทันท่วงทีหากไม่มี Dashboard
- **Threat Intelligent** คือความสามารถในการรับข้อมูลจากแหล่งรวบรวมข้อมูลภัยคุกคาม (Threat Management) จาก Internet ข้อมูลดังกล่าวก็อย่างเช่น รายการ IP ที่ถูก Black list รูปแบบการเรียกใช้ข้อมูลผ่าน URL ที่เป็นอันตราย รวมทั้งช่องโหว่ที่มีผู้แจ้งเอาไว้ SIEM นำมาข้อมูลดังกล่าวมาประมวลผลร่วมกับ Correlation เพื่อคัดกรองหาร่องรอยหรือแนวโน้มภัยคุกคามสารสนเทศหรือช่องโหว่ นอกจาก Treat Intelligent ของผู้ผลิตบางราย ยังสามารถให้คำแนะนำในการแก้ไขช่องโหว่หรือภัยคุกคามที่ตรวจพบจากข้อมูล log ได้
- **Incident Management** มีความสามารถในการจัดการ Incident ที่เกิดขึ้น กล่าวคือเมื่อ Correlation ตรวจพบข้อมูลสอดคล้องตามเงื่อนไขที่กำหนดก็จะนำไปสร้างเป็นรายการปัญหาที่ตรวจพบ (incident) ซึ่งจะต้องมีรายละเอียดของปัญหา ระดับความเร่งด่วน ระดับความความรุนแรง รวมถึงข้อมูลจำเป็นอื่น ๆ เพื่อให้ผู้ดูแลระบบ ติดตาม แก้ปัญหา และบันทึกไว้เป็นการอ้างอิงได้ต่อไป

2.6 ตัวอย่างระบบตรวจจับ Malware Cisco Umbrella

รูปที่ 2.10 แนวคิดของ Cisco Umbrella

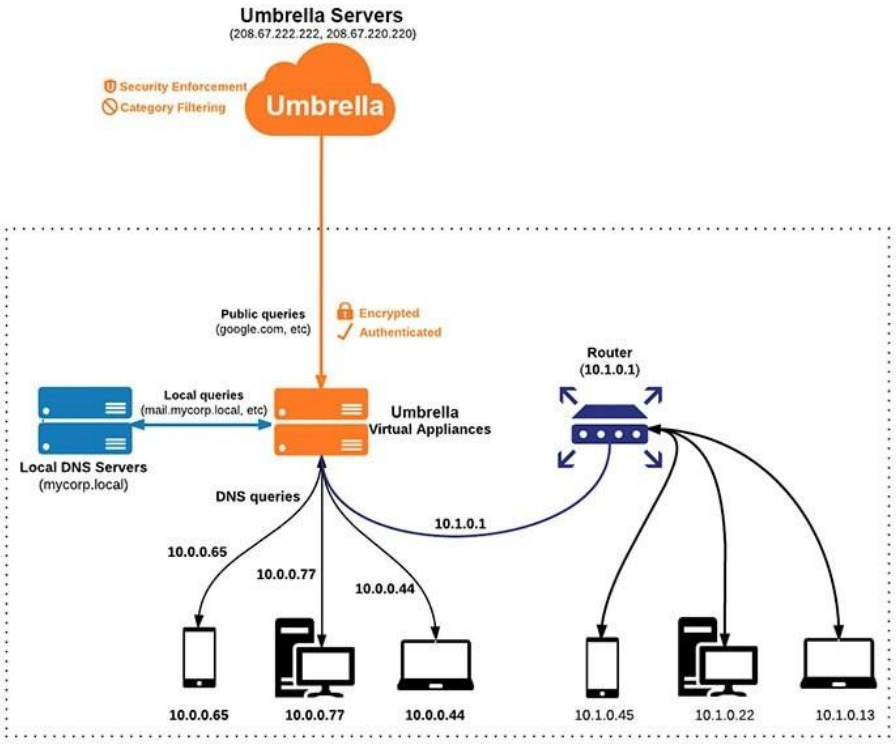
Cisco Umbrella เป็น Secure Internet Gateway (SIG) ที่ทำงานอยู่บน Cloud ดังรูปที่ 2.10 โดยมีความสามารถในการป้องกันภัยคุกคามต่างๆให้กับผู้ใช้งานที่อยู่ในองค์กรและนอกองค์กร ซึ่งสามารถตรวจสอบและจำกัดการเข้าถึง Domain, URL, IP และไฟล์ที่ไม่ปลอดภัยได้ เพื่อตอบโจทย์ทางด้านความปลอดภัยในยุคที่องค์กรเริ่มมีสาขามากขึ้นและบางสาขามีการเข้าถึง Internet โดยตรง ซึ่ง Cisco Umbrella เป็นการนำโซลูชันทางด้านความปลอดภัยต่างๆที่ Cisco มีอยู่ เช่น OpenDNS, CloudLock, Cisco AMP มาสร้างเป็นโซลูชันเพื่อตอบโจทย์กลุ่มลูกค้าองค์กร โดย Cisco Umbrella มีความสามารถเด่นดังนี้

สามารถตรวจสอบและป้องกันได้จากทุกที่ – มีเทคโนโลยี Cisco Cloudlock ซึ่งเป็น Cloud Access Security Broker ใช้ในการตรวจสอบทราฟฟิคของผู้ใช้งาน ไม่ว่าจะอยู่ภายในหรือภายนอกองค์กรตลอดเวลา เพื่อป้องกันการเข้าถึงเว็บไซท์และไฟล์ที่ไม่ปลอดภัย

สามารถหยุดการโจมตีได้ – Umbrella มีระบบตรวจสอบ Request ที่ส่งไปยัง Internet ตลอดเวลา หลัก 100 พันล้าน Request ต่อวัน และนำมาทำการเทียบเคียงกับพฤติกรรมการโจมตีในอดีตที่เก็บไว้ถึง 11 พันล้าน Events เพื่อให้สามารถตรวจจับและยับยังการโจมตีได้ก่อนที่จะเกิดขึ้น

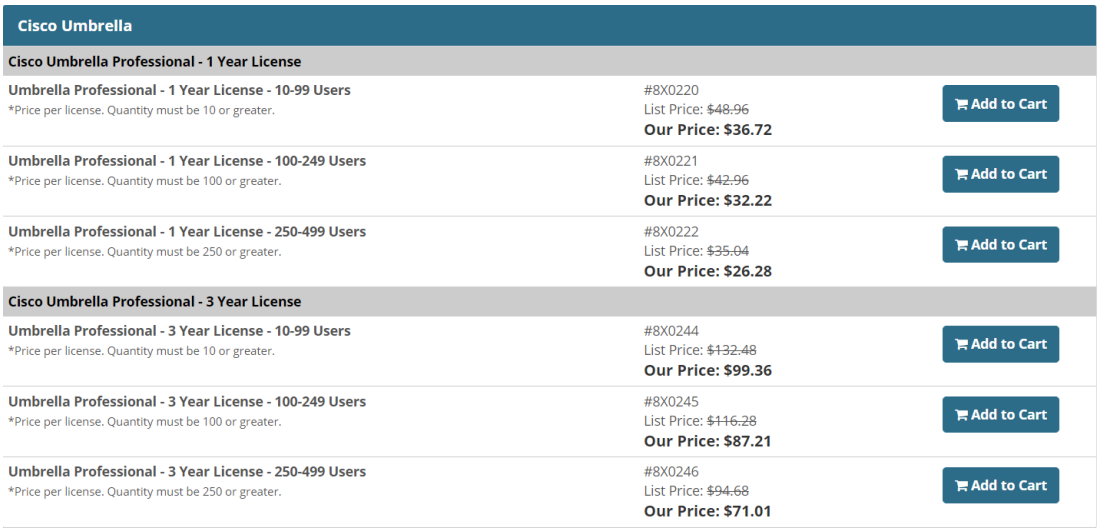
ใช้ความสามารถของระบบอื่นๆที่มีอยู่ในการตรวจจับร่วมด้วย – Cisco Umbrella นำ Machine Learning เข้ามาช่วยในการตรวจจับพฤติกรรมที่ไม่ปลอดภัย ช่วยให้สามารถตัดการเข้าถึงในระดับ DNS และ IP Layer ได้ นอกจากนี้ยังมีการนำเอาความสามารถของ Cisco Talos Threat Intelligence เพื่อใช้ในการป้องกันความเสี่ยงของ URL ที่เข้าถึงในระดับ HTTP/S อีกด้วย และยังสามารถทำงานร่วมกับ Cisco Advanced Malware Protection (AMP) ที่ใช้ในการป้องกันการเข้าถึงไฟล์ที่ไม่ปลอดภัยได้

เป็นระบบ Open Platform – รองรับการทำงานร่วมกับระบบอื่นๆที่องค์กรมีอยู่ได้ทันที เช่น ระบบ Security Monitoring ต่างๆ



รูปที่ 2.11 ตัวอย่างการติดตั้งของ Cisco Umbrella

โดยวิธีการติดตั้งนั้น จำเป็นต้องมี Umbrella Virtual Appliances ทำหน้าที่เป็น DNS local โดยให้ให้ Client ทุกเครื่องชี้ DNS มาที่ Umbrella Virtual Appliances เครื่องนี้ ดังรูปที่ 2.11 และหากหน่วยงานนั้นมีหลายสาขา จำเป็นต้องติดตั้ง Umbrella Virtual Appliances ต่อ 1 สาขา ซึ่งค่าใช้จ่ายสำหรับ Cisco Umbrella นั้น อาจจะต้องใช้เงินเป็นจำนวนมากดังรูปที่ 2.12



Cisco Umbrella		
Cisco Umbrella Professional - 1 Year License		
Umbrella Professional - 1 Year License - 10-99 Users *Price per license. Quantity must be 10 or greater.	#8X0220 List Price: ~~$48.96~~ **Our Price: $36.72**	Add to Cart
Umbrella Professional - 1 Year License - 100-249 Users *Price per license. Quantity must be 100 or greater.	#8X0221 List Price: ~~$42.96~~ **Our Price: $32.22**	Add to Cart
Umbrella Professional - 1 Year License - 250-499 Users *Price per license. Quantity must be 250 or greater.	#8X0222 List Price: ~~$35.04~~ **Our Price: $26.28**	Add to Cart
Cisco Umbrella Professional - 3 Year License		
Umbrella Professional - 3 Year License - 10-99 Users *Price per license. Quantity must be 10 or greater.	#8X0244 List Price: ~~$132.48~~ **Our Price: $99.36**	Add to Cart
Umbrella Professional - 3 Year License - 100-249 Users *Price per license. Quantity must be 100 or greater.	#8X0245 List Price: ~~$116.28~~ **Our Price: $87.21**	Add to Cart
Umbrella Professional - 3 Year License - 250-499 Users *Price per license. Quantity must be 250 or greater.	#8X0246 List Price: ~~$94.68~~ **Our Price: $71.01**	Add to Cart

รูปที่ 2.12 ราคา price list ของ Cisco Umbrella

บทที่ 3

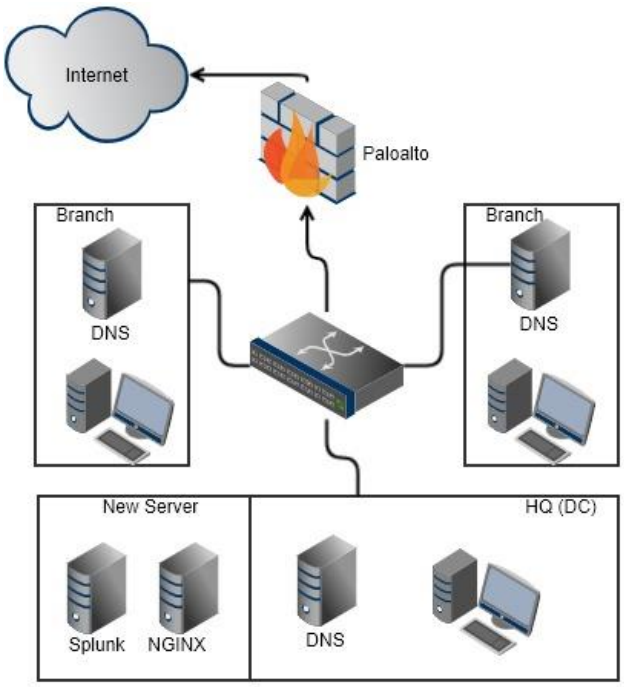
ระบบที่นำเสนอ

3.1 ภาพรวมและโครงสร้างของระบบ

จากโครงสร้างระบบเครือข่ายภายในหน่วยงาน จะแสดงให้เห็นดังรูป 3.1 แต่ละสาขาจะสามารถติดต่อกับ Data Center ได้ และแต่ละสาขาจะมี DNS Server ประจำสาขาโดยที DNS ที่สาขาจะแลกเปลี่ยน Record ของ DNS ตามช่วงเวลาที่กำหนด

ที่ Data Center จะมี Firewall วางขวาง Data Center ไว้ และภายใน Data Center จะมี DNS Server และได้ออกแบบให้มี Server เพิ่ม 2 เครื่องได้แก่ NGINX ทำหน้าที่เป็น Reverse Proxy ไว้สำหรับดักจับและรับ Traffic ที่มัลแวร์จะพยายามติดต่อไปยัง C&C Server และ Splunk ทำหน้าที่รับ Log จาก NGINX เพื่อไปวิเคราะห์ยืนยันเครื่องที่ถูกติดตั้งมัลแวร์และสามารถส่ง Email แจ้งเตือนเพื่อให้สามารถตอบสนองและรับมือกับมัลแวร์ได้รวดเร็วขึ้น

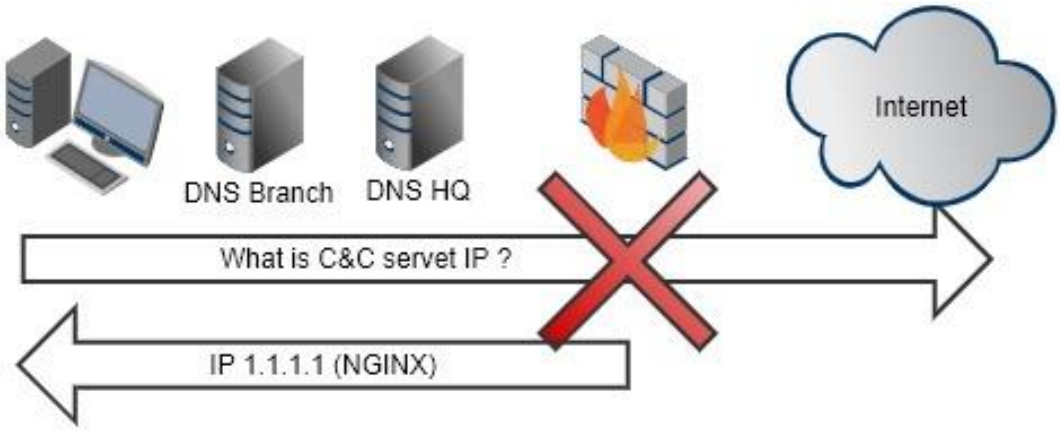
ที่ Internet zone จะมี Paloalto ซึ่งเป็นอุปกรณ์ Next-Generation Firewall วางขวางก่อนจะออกไปยัง Internet zone ทำให้ Traffic ก่อนทีจะถึง Public DNS จะต้องผ่าน Paloalto ก่อนเสมอ



รูปที่ 3.1 Network Diagram

3.2 การทำงานของ Next-Generation Firewall ภายในระบบ

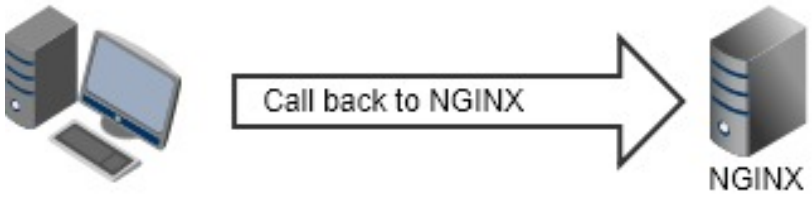
เมื่อคอมพิวเตอร์ตามสาขาซึ่งถูกติดตั้งมัลแวร์ไว้ได้พยายามติดต่อไปยัง C&C Server โดยที่มัลแวร์ส่วนใหญ่จะเรียกไปที่ C&C Server ด้วย DNS แทนการเรียกเป็น IP ตรงๆ ซึ่งสามารถหลบเลี่ยง Firewall ธรรมดาที่ Block Traffic เฉพาะ IP ได้ เมื่อมัลแวร์เริ่ม Query DNS จะติดต่อไปยัง DNS Server ที่อยู่ที่สาขาก่อนเป็นอันดับแรก หากไม่มี Record DNS จะส่งต่อไปที่ DNS Server ที่ Data Center ซึ่ง Traffic ที่ Query DNS จะผ่านไปเช็ค Record DNS ที่ DNS Server ภายใน Data Center หลังจากนั้นจะถูกส่งต่อไปที่ DNS ที่ Public DNS ซึ่ง Traffic ที่ Query DNS จะผ่านอุปกรณ์ Paloalto ซึ่งหาก DNS ที่ Query นั้นไม่อยู่ใน Blacklist ของอุปกรณ์ Paloalto Traffic จะถูกปล่อยผ่านไปหา Root DNS Servers ตามกระบวนการ DNS ปกติ แต่หากอยู่ใน Blacklist ของอุปกรณ์ Paloalto DNS จะถูกตอบกลับเป็น IP ที่กำหนดขึ้นมาได้ ทั้งนี้ได้ออกแบบให้ตอบกลับเป็น IP ของ NginX เพื่อหลอกให้มัลแวร์ไปติดต่อกับ NginX แทน C&C Server ดังรูปที่ 3.2



รูปที่ 3.2 แสดงการตอบกลับของ Blacklist Domain

3.3 การทำงานของ Reverse Proxy ภายในระบบ

หลังจากที่มัลแวร์ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ ได้ IP ของ C&C Server ที่เป็น NGINX แทนที่มัลแวร์จะติดต่อไปยัง C&C Server แต่ถูกเปลี่ยนให้ติดต่อไปยัง NGINX แทนดังรูปที่ 3.3



รูปที่ 3 3 แสดงการทำงานขณะที่มัลแวร์เรียกไปยัง C&C Server

เมื่อ Traffic ของเครื่องคอมพิวเตอร์มายัง NGINX ทุก Traffic จะถูก log ไว้เก็บไว้ ทุก Parameters จะถูกบันทึกไว้เช่นกัน หาก Protocal ที่ใช้ไม่ใช่ Protocol HTTP ที่ NGINX ยังสามารถ Log ในส่วนของ Request ได้ ยังสามารถเอาไปวิเคราะห์ได้ต่อว่าเป็น Traffic หรือ Payload ประเภทไหนได้เช่นกัน

3.4 การทำงานของ SIEM ในระบบ

หลังจากที่มัลแวร์ติดต่อไปยัง C&C Server ที่เป็น NGINX แล้วจะเกิด Access Log ที่ NGINX ให้ส่ง Access Log ไปที่ Splunk ที่ทำหน้าที่เป็น SIEM ด้วย Syslog UDP 514 เพื่อนำ Log ไปวิเคราะห์และ Report ไปที่ Admin ดังรูปที่ 3.4

รูปที่ 3.4 แสดงการรับ Log และส่ง Report ไปยัง Admin

จาก Log ที่เกิดขึ้นหากพบว่ามีคอมพิวเตอร์ IP ไหนติดต่อมายัง NGINX เป็นการยืนยันได้ว่าเครื่องคอมพิวเตอร์ IP ดังกล่าวถูกติดตั้งมัลแวร์ไว้และวิธีตรวจสอบ IP เครื่องคอมพิวเตอร์ดังกล่าวแบ่งเป็น 2 ประเภทคือ

- IP ต้นทางที่พยายามติดต่อมาโดยไม่ผ่าน Proxy ของหน่วยงาน จะสามารถดูได้จาก IP ต้นทางที่ติดต่อมา
- IP ต้นทางที่เรียกผ่าน Proxy ของหน่วยงาน จะสามารถดู IP ต้นทางได้จาก X-Forwarded-For เป็น Header ของ Protocol HTTP ที่ Proxy ของหน่วยงานเพิ่มเข้ามา

เมื่อยืนยัน IP เครื่องคอมพิวเตอร์ต้นทางได้แล้ว ต้องมาวิเคราะห์ต่อว่าเครื่องคอมพิวเตอร์ดังกล่าวติดตังมัลแวร์ตัวไหนและประเภทอะไร โดยเริ่มจากมัลแวร์ติดต่อไปยัง C&C Server อะไร ซึ่งสามารถ Filter ในส่วนของ Domain ของ Malware ได้ หลังจากนั้นจะแยกขั้นตอนอีก 2 แบบคือ

- มัลแวร์ตัวไหนที่ติดต่อกับ C&C Server ด้วย Protocol HTTP/HTTPS สามารถตรวจสอบกับ Hostname ที่มัลแวร์เรียกออกไป จะสามารถระบุได้ว่า เครื่องคอมพิวเตอร์ IP ดังกล่าวติดตั้งมัลแวร์ตัวไหน ประเภทอะไร โดยสามารถหาข้อมูลเพิ่มเติมได้จาก Third Party ได้ เช่น Virustotal เป็นต้น
- มัลแวร์ตัวไหนที่ติดต่อกับ C&C Server ที่ไม่ใช้ Protocol HTTP/HTTPS จะมีความซับซ้อนในการตรวจหาชนิดของมัลแวร์มาก โดยต้องตรวจสอบให้ได้ก่อนว่าเป็น Payload ประเภทไหน แล้วค่อยหาข้อมูลเพิ่มเติมว่า มัลแวร์ตัวไหนใช้ Payload ชนิดนี้

บทที่ 4

ผลการดำเนินงาน

4.1 บทนำ

จากผลการดำเนินงานได้มีการทำการทดสอบระบบตรวจจับมัลแวร์ โดยเข้าไปดูในระบบ ซึ่งในหน้า Dash board จะระบุไว้ว่า C&C Domain ไหนบ้างที่มีเครื่องลูกข่ายติดต่อไป แบบ Real-Time และมี Report ที่สามารถสรุปเป็นรายวันได้

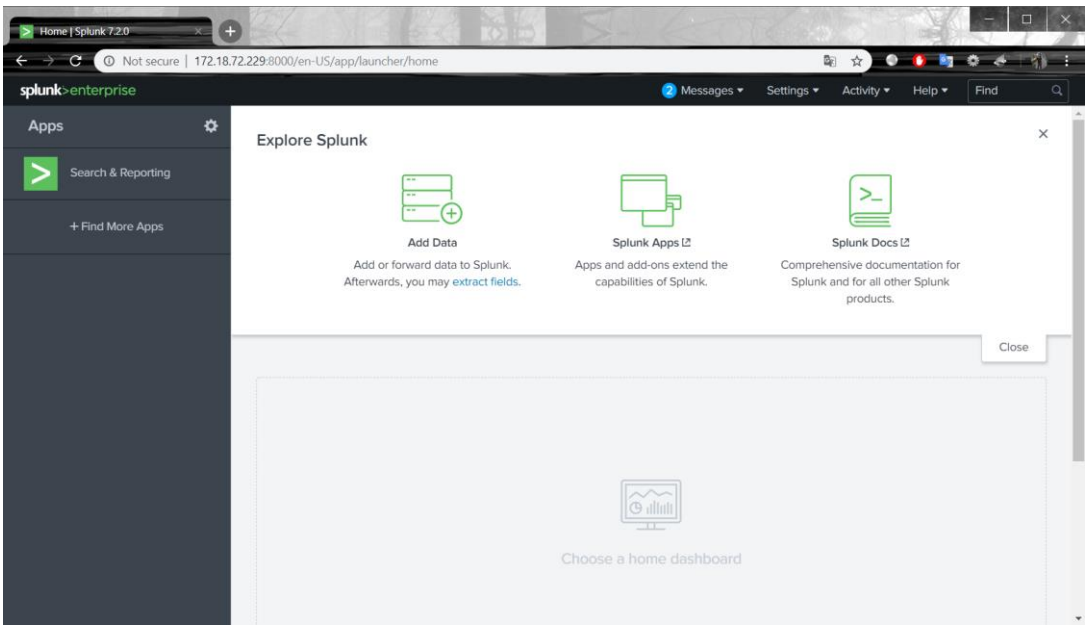
เพื่อที่จะยืนยันได้ว่า ผลการทดสอบนั้นเป็นจริง จึงต้องทำการสำรวจหมายเลข IP ที่มีใน Report เพื่อพิสูจน์ว่า เครื่องดังกล่าวเป็นเครื่องที่ติดมัลแวร์

4.2 ผลการดำเนินงาน

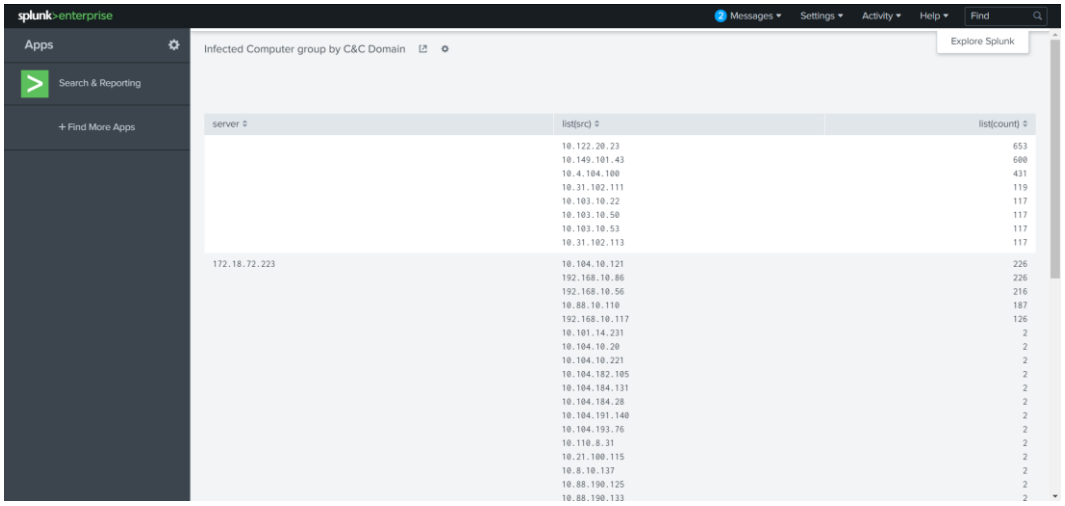
4.2.1 Dash Board จากระบบ Splunk

จากผลการทดสอบนำ Log จาก NGINX ส่งเข้าไปยัง Splunk และใช้ Splunk ในการทำ Dash Board ผลการดำเนินงานมีดังต่อไปนี้

เข้าสู่ระบบ Slunk ที่หน้าแรกจะพบกับหน้า Dash Board ซึ่งจะระบุว่า C&C Domain ไหนบ้างที่มีเครื่องลูกข่ายติดต่อไป ดังรูปที่ 4.1 และ รูปที่ 4.2



รูปที่ 4.1 หน้าแรกของระบบ Splunk

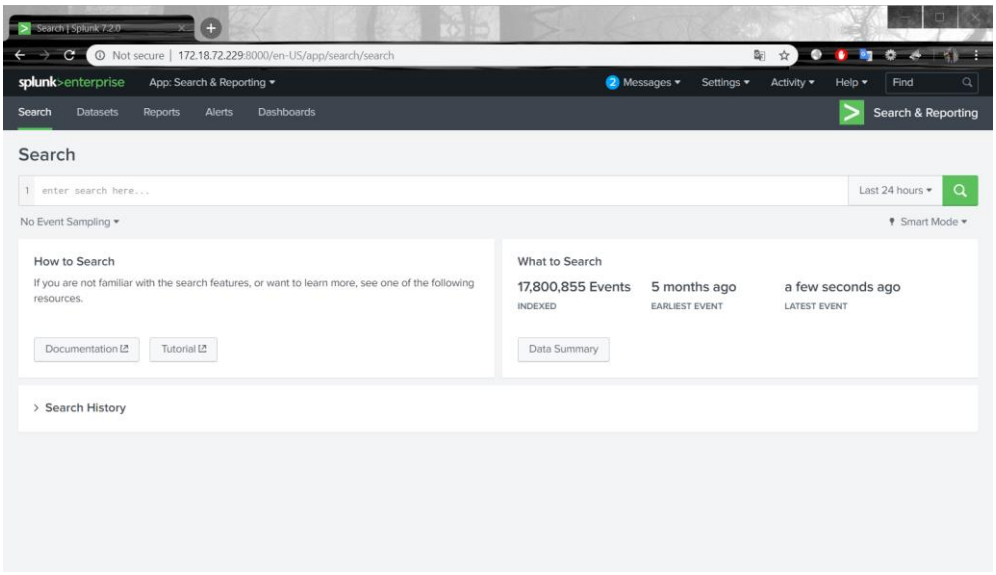


รูปที่ 4.2 หน้า Dash Board ของระบบ Splunk

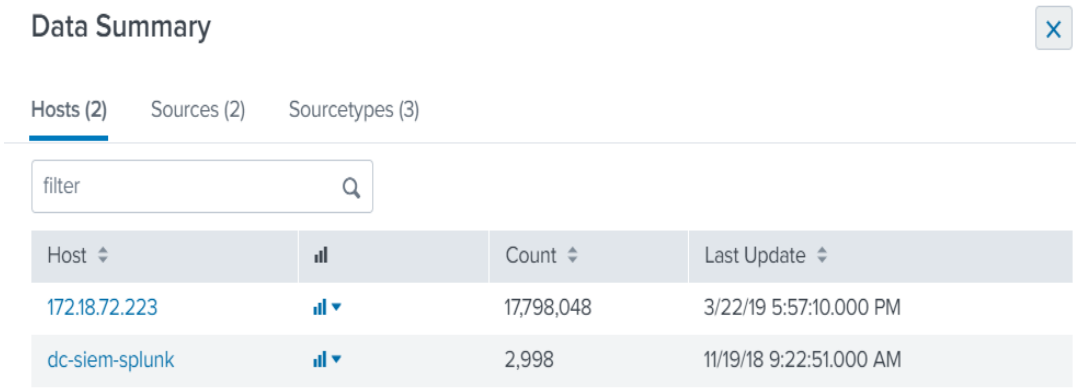
4.2.2 Report จากระบบ Splunk

จากผลการทดสอบนำ Log จาก NGINX ส่งเข้าไปยัง Splunk และใช้ Splunk ในการทำ Report ผลการดำเนินงานมีดังต่อไปนี้

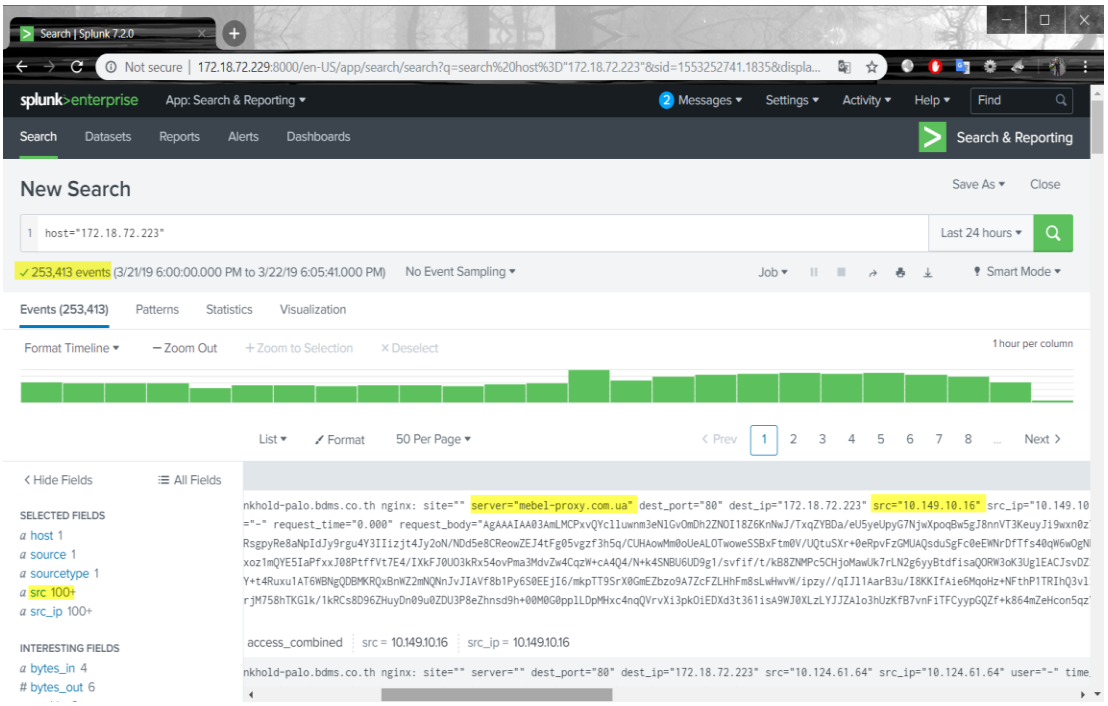
เข้าสู่ระบบ Slunk จากนั้นเข้าไปที่ Search & Report ดังรูปที่ 4.3 แล้วคลิ๊กที่ Data Summary เลือก 172.18.72.223 ซึ่งเป็น IP ของ NGINX ที่ส่ง Log เข้ามา ดังรูปที่ 4.4 จะพบหน้า Search Log ของ Splunk ดังรูปที่ 4.5



รูปที่ 4.3 หน้า Search ของระบบ Splunk



รูปที่ 4.4 หน้า Data Sumarry ของระบบ Splunk

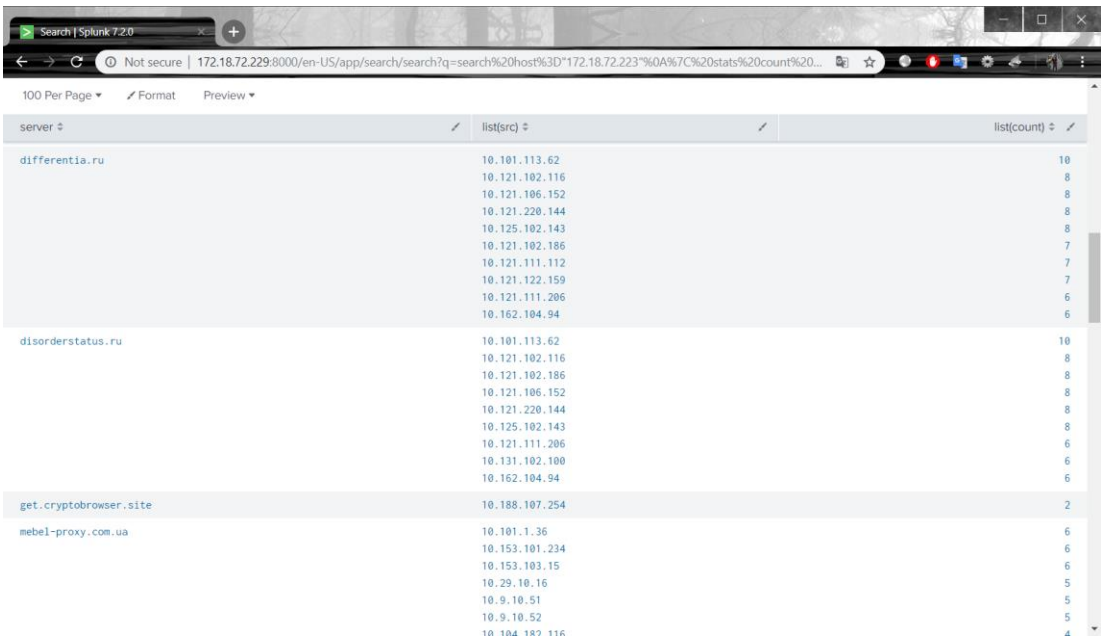


รูปที่ 4.5 หน้า Search ของ Splunk

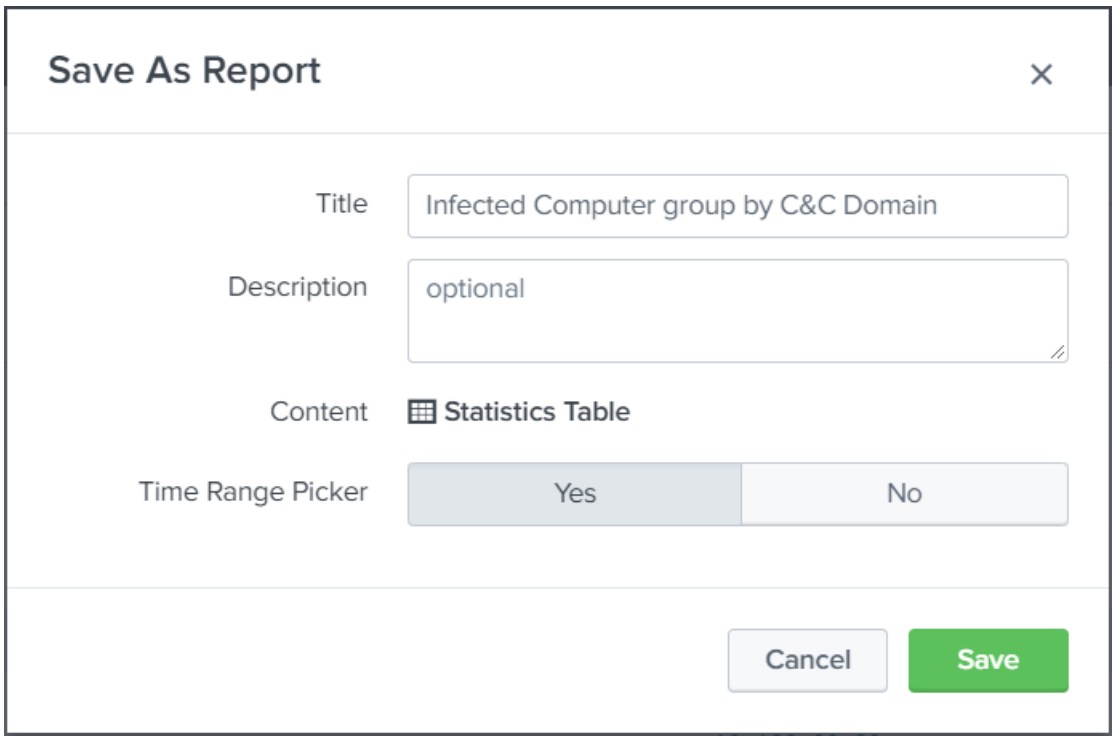
จากหน้า Search จะพบว่ามี Log จำนวนมากถูกส่งมาจาก NGINX จากหน้านี้จะสามารถบอกจำนวนเครื่องที่ติดมัลแวร์ได้คร่าวๆจากจำนวน src ทางด้านซ้ายมือ ซึ่งในที่นี้บอกว่ามีจำนวนมากกว่า 100 เครื่อง

ใน Log ที่ถูกส่งมานั้นสิ่งที่น่าสนใจใน Log ก็คือ server ซึ่งหมายถึง C&C Server และ src หมายถึงเครื่องที่ติดมัลแวร์ ดังนั้นจึง Query ข้อมูลเอาเฉพาะ server กับ src มาจับคู่กันจะได้ดังรูปที่ 4.6 และรูปที่ 4.7 และสร้างเป็น Report ขึ้นมาดังรูปที่ 4.8 และ รูปที่ 4.9

รูปที่ 4.6 การ Query Log บน Splunk



รูปที่ 4.7 ผลจากการ Query Query Log บน Splunk



รูปที่ 4.8 สร้าง Report


Infected Computer group by C&C Domain

server	list(src)	list(count)
	10.118.114.172	3206
	10.122.20.23	2564
	10.154.61.173	2404
	10.126.106.43	2315
	10.101.1.199	2268
	10.124.61.64	2129
	10.102.103.185	1486
	10.149.101.43	1399
	10.118.102.152	1383
	10.150.111.142	1332
	10.4.104.100	531
	10.103.10.22	481
	10.103.10.50	481
	10.103.10.53	481
	10.31.102.111	481
	10.31.102.113	481
	10.112.32.177	105
	10.88.129.109	30
	10.101.113.150	1
	10.106.101.48	1
	10.126.101.32	1
	10.104.10.121	488
	192.168.10.56	437
	10.11.1.21	432
	10.88.10.71	431
	192.168.10.86	431
	10.104.10.13	430
	10.11.1.29	345
	10.110.10.7	243
	10.155.106.31	238
	10.88.10.110	225
	10.1.106.230	223
	192.168.10.31	220
	10.88.10.93	218
	10.88.10.96	216
	10.88.10.69	215
	10.88.10.85	215
	192.168.10.117	215
	192.168.10.190	215
	10.11.1.33	45
	10.104.10.20	8
	10.104.10.221	8
	10.104.182.105	8
	10.104.184.28	8
	10.104.191.140	8
	10.104.193.76	8
	10.110.8.31	8
	10.146.103.55	8
	10.21.100.115	8
	10.8.10.137	8
	10.88.190.125	8
	10.88.190.133	8
	172.18.8.25	8
	10.101.14.231	7
	10.153.109.45	7
	10.118.102.111	4
	10.88.193.159	3
172.18.72.223	10.146.61.43	1
adblock.qhuweb.com	10.161.67.253	2

รูปที่ 4.9 ตัวอย่างไฟล์ PDF ของ Report

4.2.3 การสำรวจและพิสูจน์หามัลแวร์

หลังจากที่ได้ข้อมูลจาก Splunk จึงได้ดำเนินการสำรวจจำนวนทั้งหมดจำนวน 8 เครื่อง แยกตาม C&C Server ได้ 5 Domain ดังตาราง 4.1

ตารางที่ 4.1 รายชื่อ C&C Server กับ IP คอมพิวเตอร์ที่จะสำรวจ

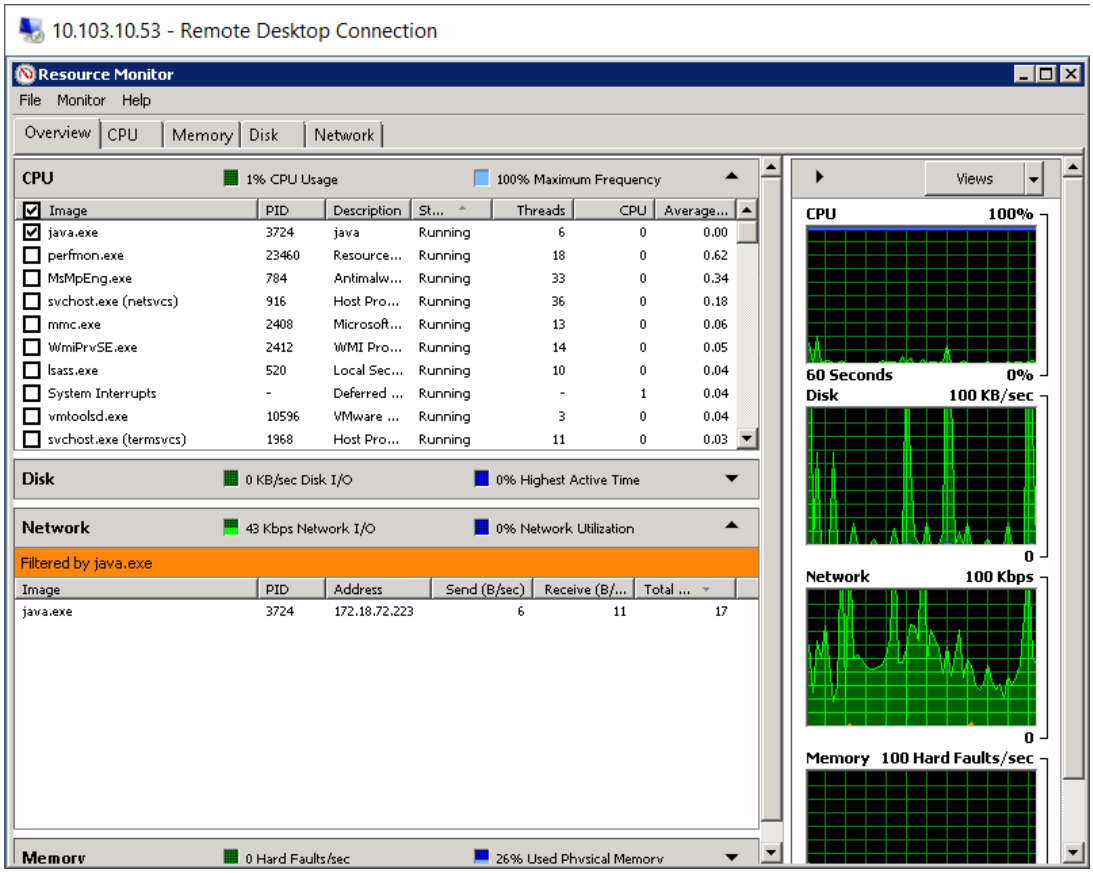
C&C Server	IP ของเครื่องที่ติดมัลแวร์ใน Report
Null	10.103.10.53
	10.103.10.22
differentia.ru	10.88.154.164
disorderstatus.ru	10.131.102.100
mebel-proxy.com.ua	10.134.10.54
	10.153.103.15
cdnrep.reimage.com	10.148.103.146
	10.148.102.181

1) C&C Server : Null และ IP : 10.103.10.53

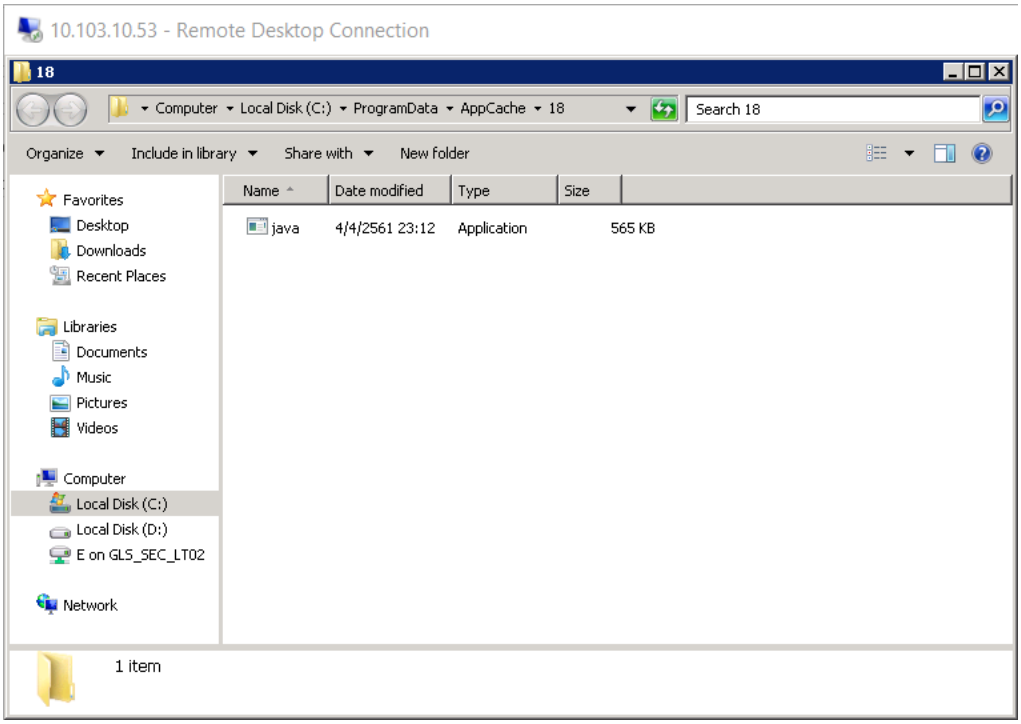
จากข้อมูลใน Report พบว่า C&C Server ไม่มีข้อมูลเพราะว่า Protocal ที่ใช้ติดต่อกลับไปยัง C&C Server ไม่ใช่ HTTP Protocal จึงระบุไม่ได้ว่า C&C Server เป็น Domain อะไรดังรูปที่ 4.10

รูปที่ 4.10 ตัวอย่าง Log จาก IP 10.103.10.53

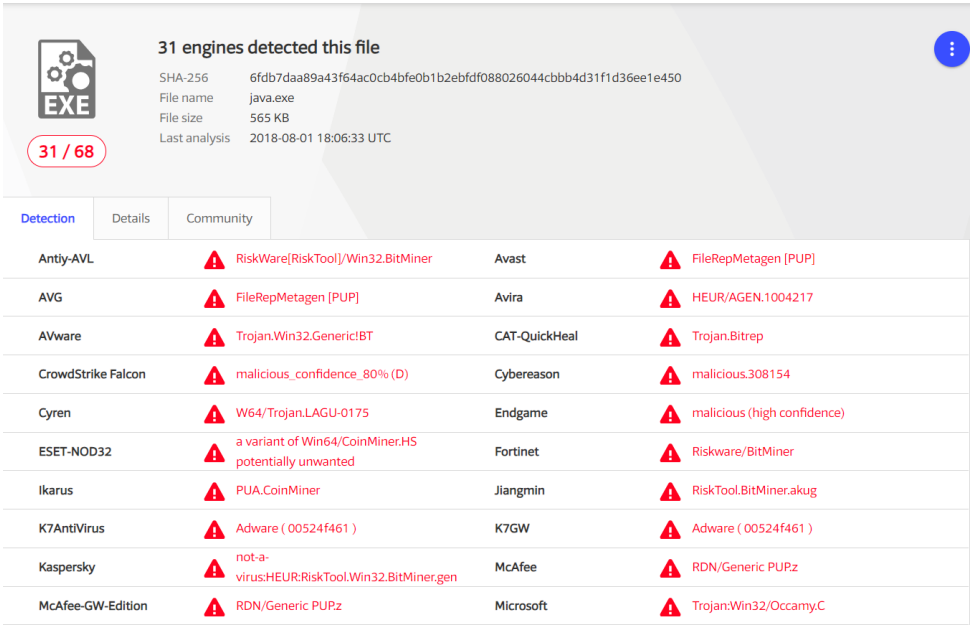
เมื่อ Remote เข้าไปที่เครื่องพบว่ามีการเชื่อมต่อมายัง NGINX (172.18.72.223) ด้วย Process Java ดังรูปที่ 4.11 และเมื่อนำไฟล์ดังกล่าวตรวจสอบกับ Virustotal พบว่าเป็นมัลแวร์ประเภท Trojan.Bitminer ดังรูปที่ 4.12 และ 4.13 ซึ่งแก้ไขได้โดยการติดตั้ง Anti-Virus และอัพเดต Signature ให้เป็นปัจจุบันและสั่ง Full-Scan เครื่องคอมพิวเตอร์และหลังจากนั้น Restart เครื่อง



รูปที่ 4 11 Process Java ติดต่อมายัง NGINX (172.18.72.223)



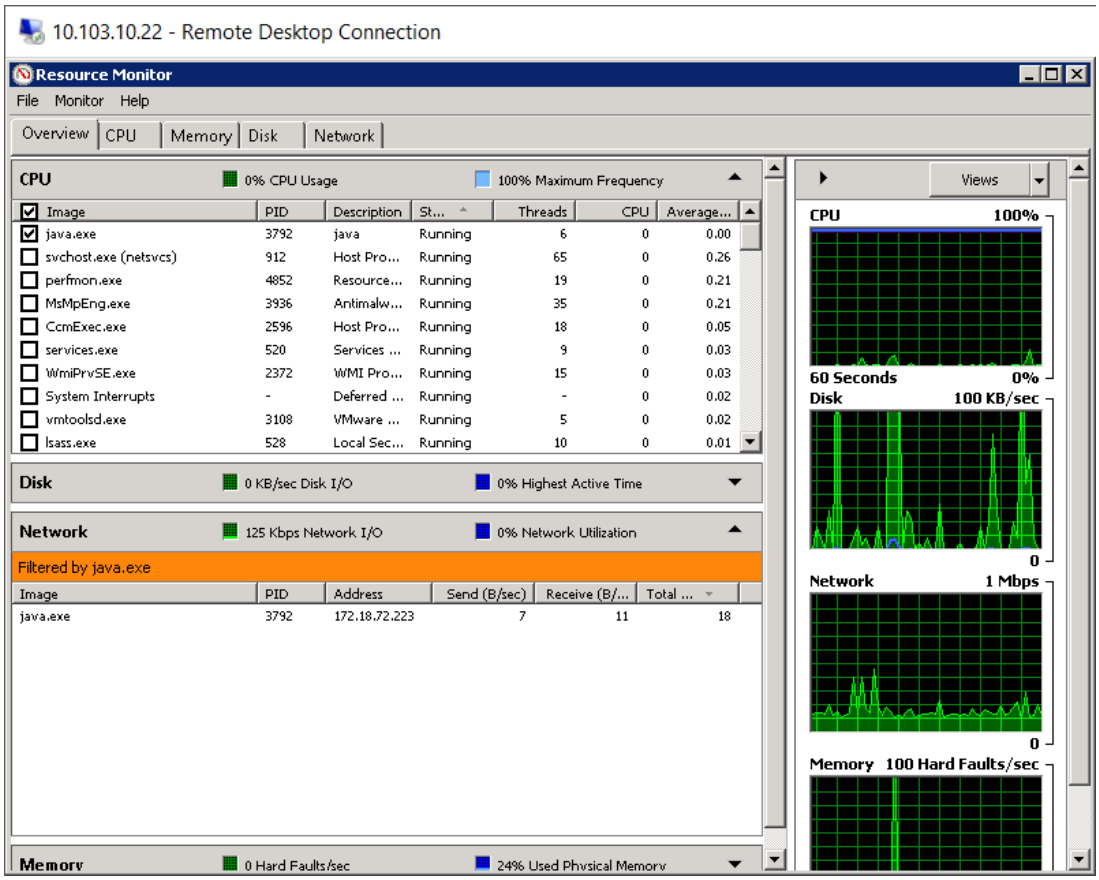
รูปที่ 4.12 ไฟล์ java ที่ติดต่อไปยัง NGINX



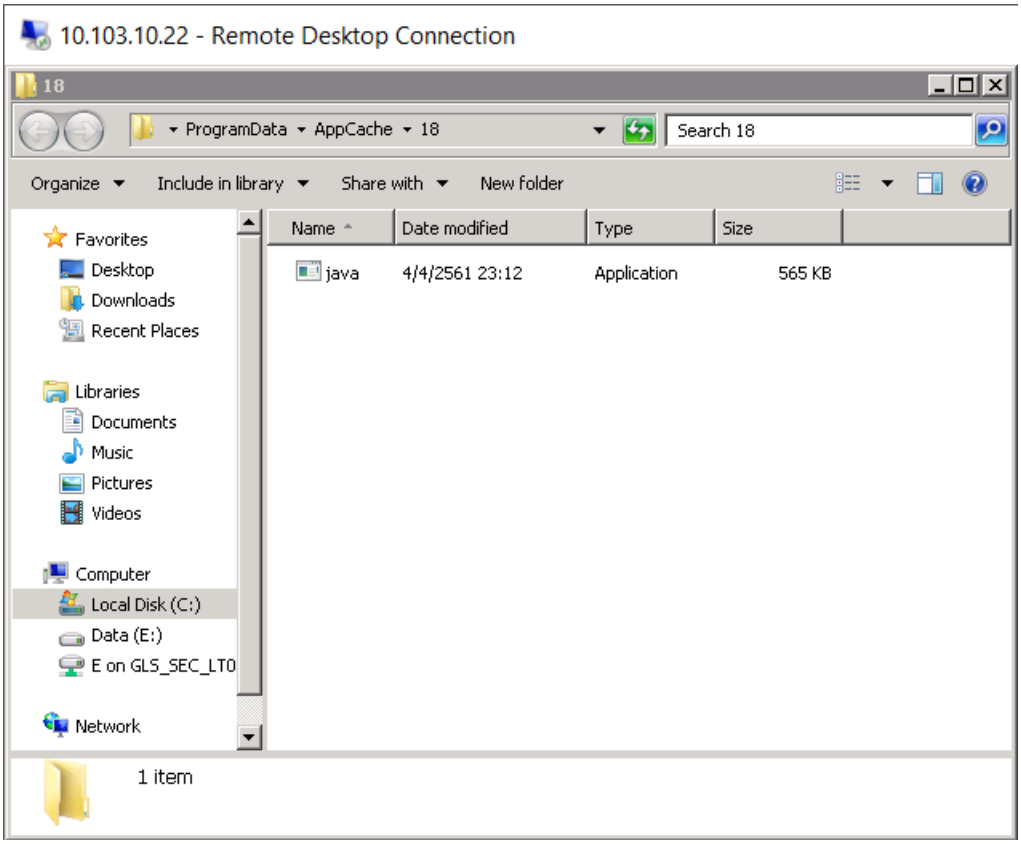
รูปที่ 4.13 Virustotal แจ้งว่าเป็นมัลแวร์

2) C&C Server : Null และ IP : 10.103.10.22

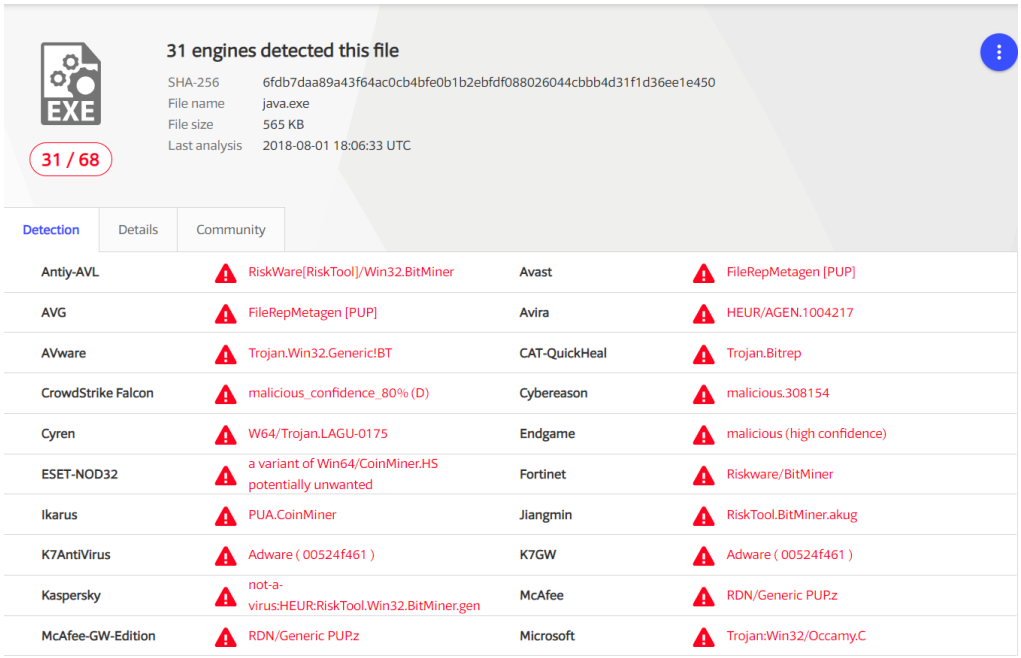
เนื่องจาก C&C Server เป็นค่า Null เหมือนกัน และ Log ใกล้เคียงกันมาก ผลการสำรสจเหมือนกันทุกประการดังรูปที่ 4.14, 4.15 และ 4.16 ซึ่งแก้ไขได้โดยการติดตั้ง Anti-Virus และอัพเดต Signature ให้เป็นปัจจุบันและสั่ง Full-Scan เครื่องคอมพิวเตอร์และหลังจากนั้น Restart เครื่อง



รูปที่ 4.14 Process Java ติดต่อมายัง NGINX (172.18.72.223)



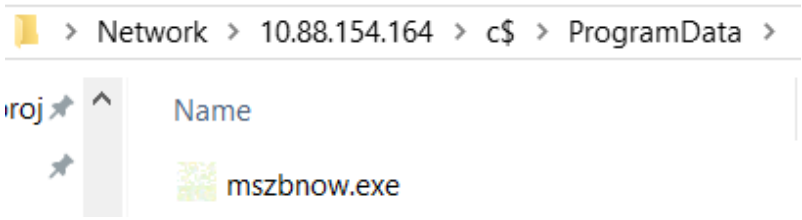
รูปที่ 4.15 ไฟล์ java ที่ติดต่อไปยัง NGINX



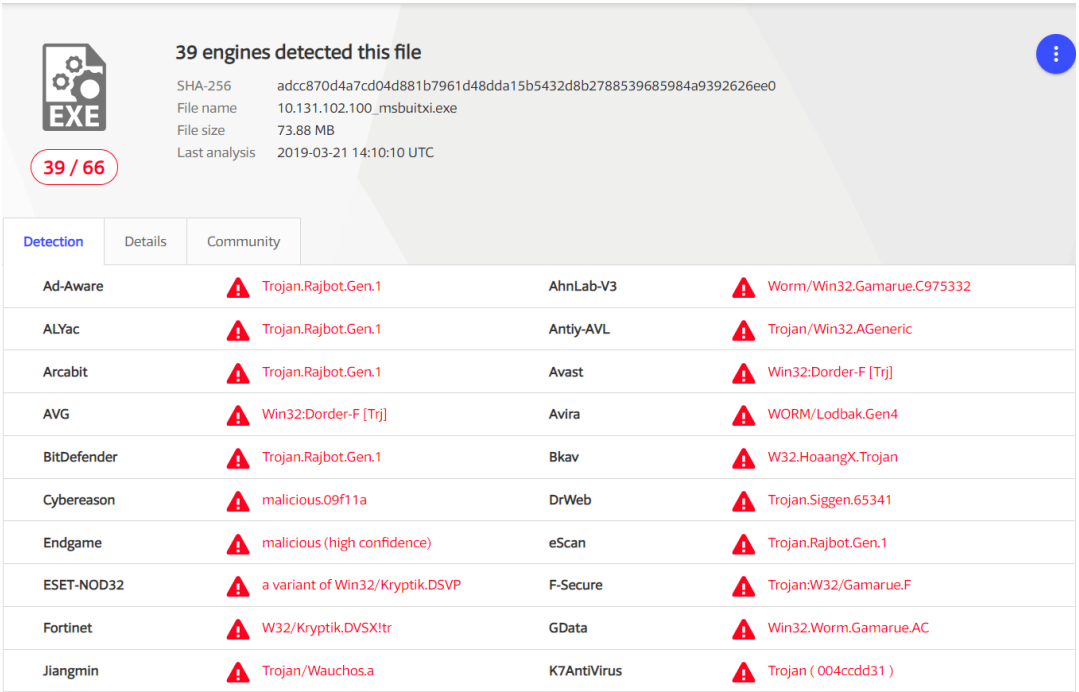
รูปที่ 4.16 Virustotal แจ้งว่าเป็นมัลแวร์

3) C&C Server : differentia.ru และ IP : 10.88.154.164

จากการสืบค้นข้อมูลพบว่า C&C Server : differentia.ru นั้นมีมัลแวลร์ที่ชื่อว่า Andomeda เรียกกลับไป ซึ่งพฤติกรรมของมัลแวร์ตัวนี้จะสร้างไฟล์ไว้ที่ C:/ProgramData/ สำหรับ Windows7 ขึ้นไปและ C:/Documents and Settings/All User สำหรับ Windows ที่ต่ำกว่า Windows 7 โดยลักษณะของชื่อไฟล์จะขึ้นต้นด้วย ms ตามด้วยสุ่มตัวอักษรอีก 6 ตัว ดังรูปที่ 4.17 และเมื่อนำไฟล์ดังกล่าวไปเช็คกับ Virustotal พบว่าไฟล์ดังกล่าวเป็น Malware ดังรูปที่ 4.18 ซึ่งแก้ไขได้โดยการติดตั้ง Anti-Virus และอัพเดต Signature ให้เป็นปัจจุบันและสั่ง Full-Scan เครื่องคอมพิวเตอร์และหลังจากนั้น Restart เครื่อง



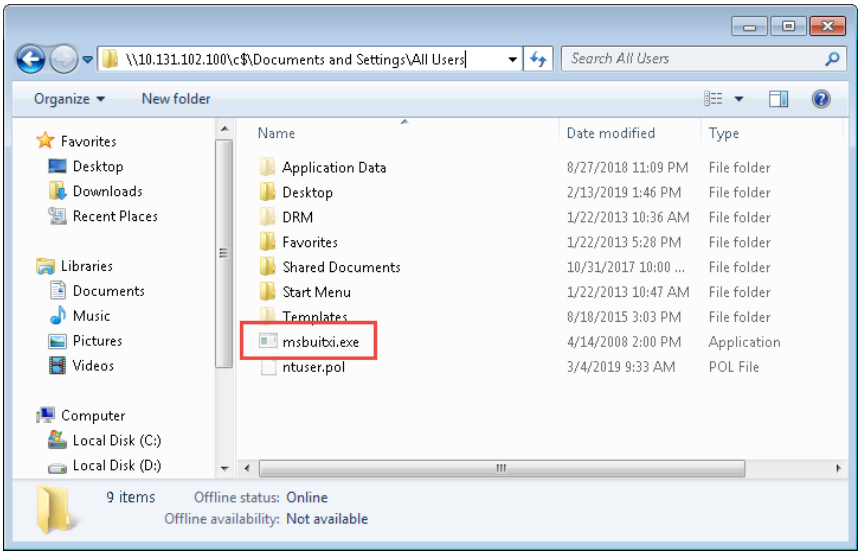
รูปที่ 4.17 ที่อยู่ของไฟล์มัลแวร์



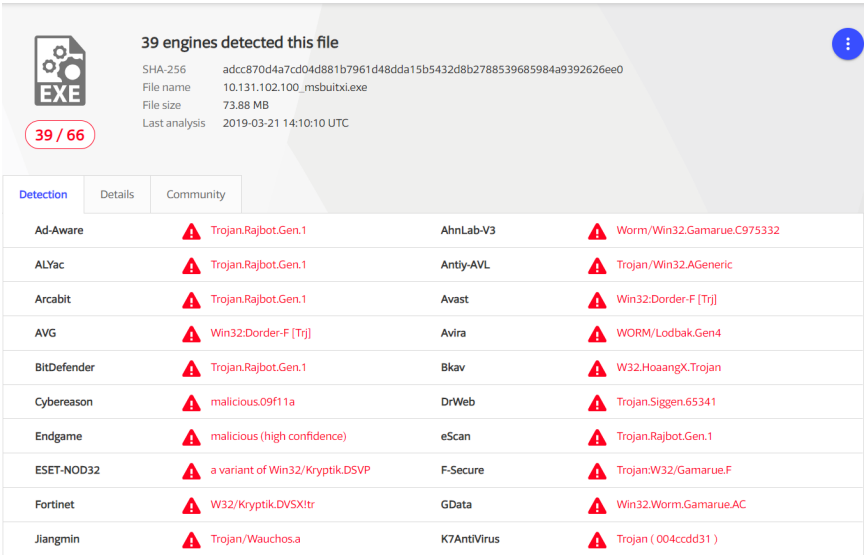
รูปที่ 4.18 Virustotal แจ้งว่าเป็นมัลแวร์

4) C&C Server : disorderstatus.ru และ IP : 10.131.102.100

จากการสืบค้นข้อมูลพบว่า C&C Server : disorderstatus.ru นั้นมีมัลแวร์ที่ชื่อว่า Andomeda เช่นเดียวกับ C&C Server: differentia.ru ดังนั้นพฤติกรรมต่างๆจะเหมือนกันทุกประการดังรูปที่ 4.19 และ 4.20



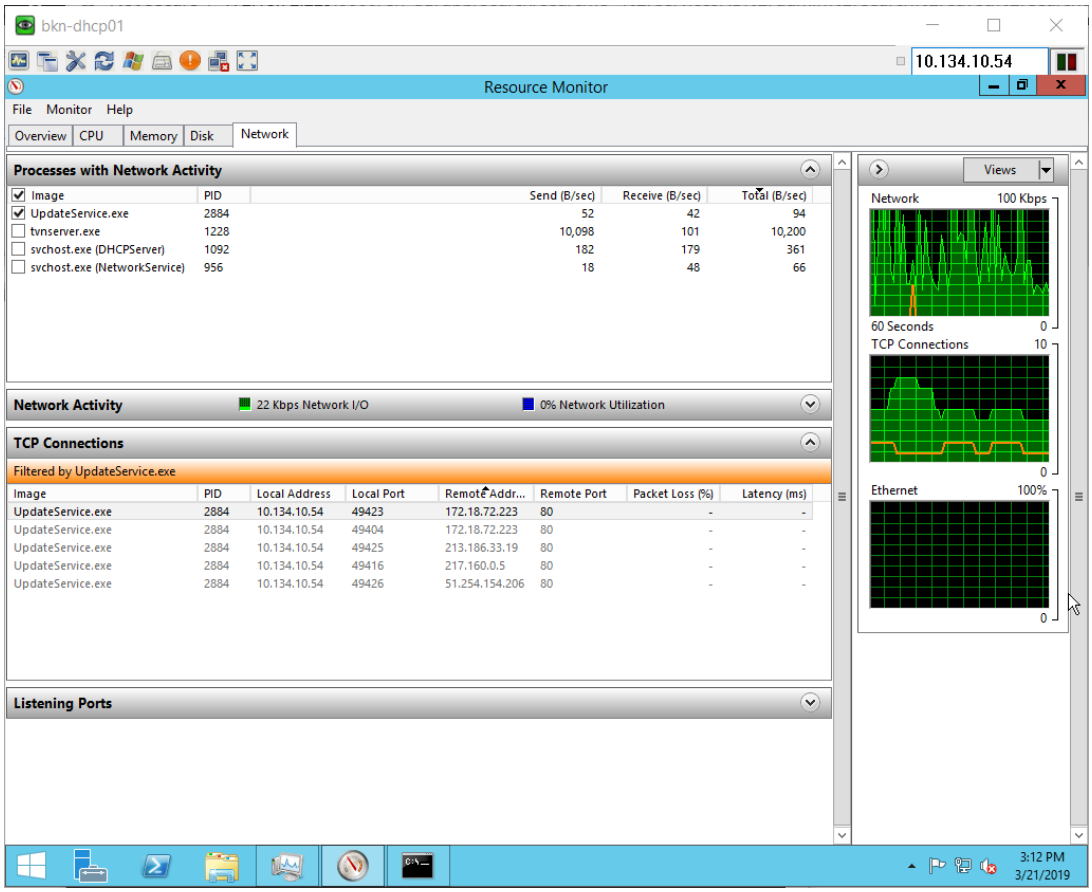
รูปที่ 4.19 ที่อยู่ของไฟล์มัลแวร์



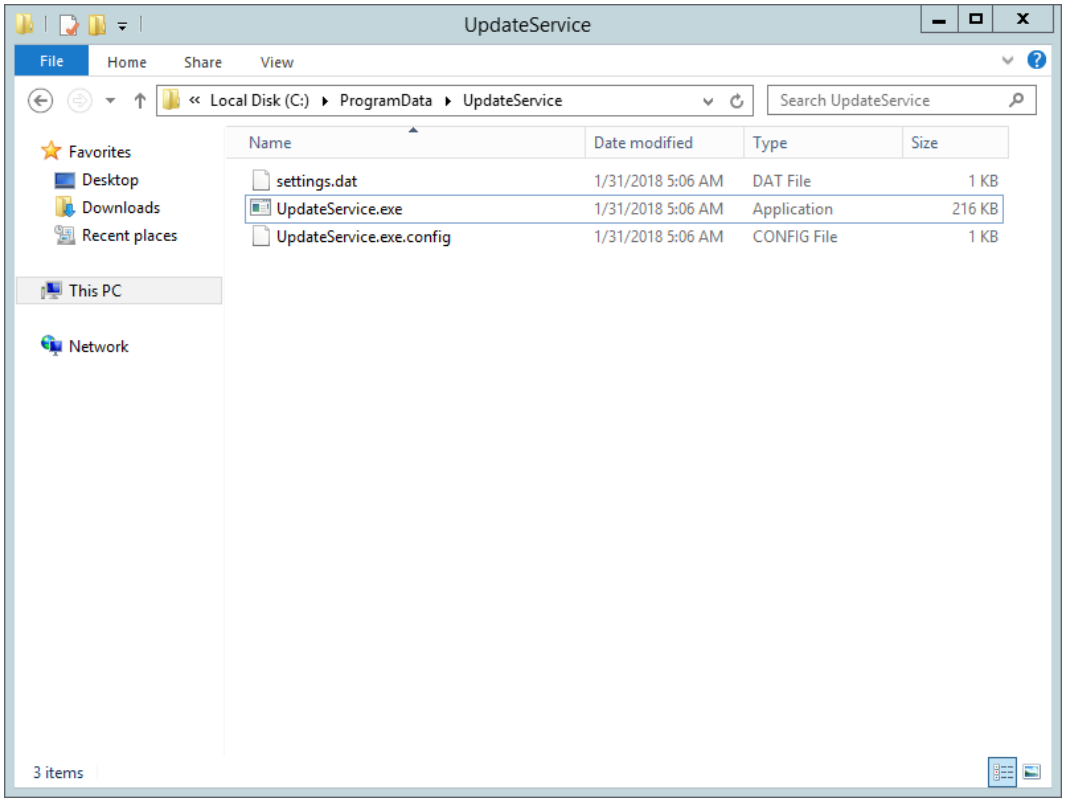
รูปที่ 4.20 Virustotal แจ้งว่าเป็นมัลแวร์

5) C&C Server : mebel-proxy.com.ua และ IP : 10.134.10.54

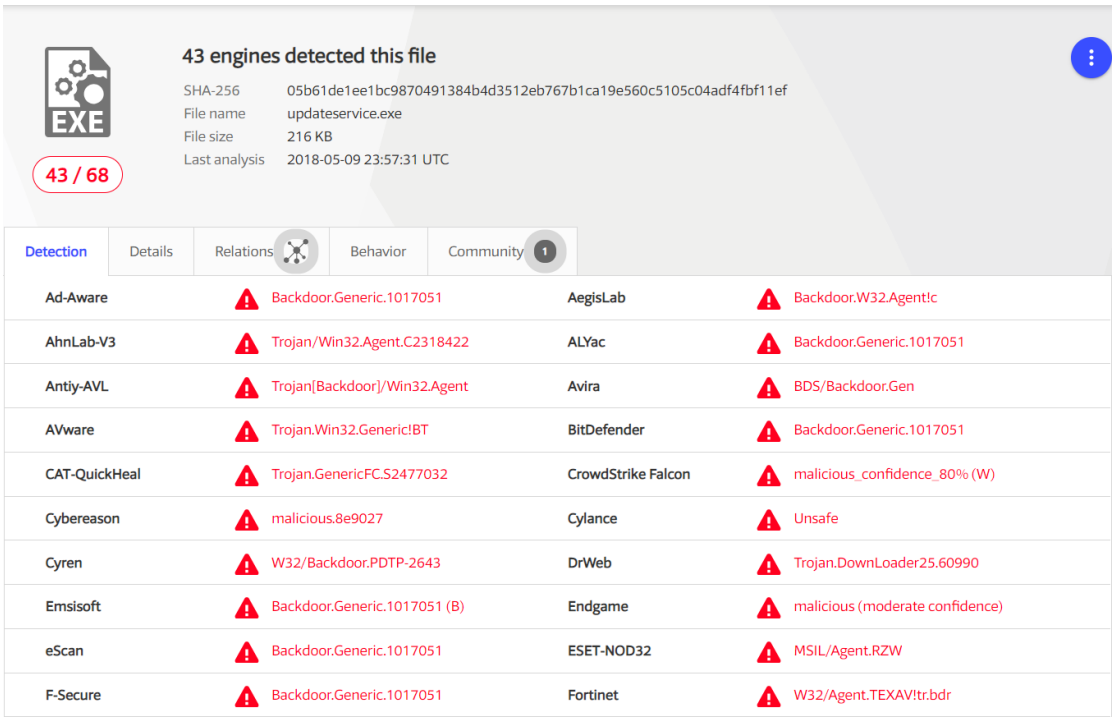
จากการสำรวจ เมื่อ Remote ไปยัง IP 10.134.10.54 พบว่า มีการเชื่อมต่อมายัง NGINX โดยเชื่อมต่อมาด้วย Process ชื่อ UpdateService.exe ดังรูปที่ 4.21 เมื่อนำไฟล์ดังกล่าวไปตรวจสอบกับ Virustotal พบว่าเป็นมัลแวร์ ดังรูปที่ 4.22 และ 4.23 ซึ่งแก้ไขได้โดยการติดตั้ง Anti-Virus และอัพเดต Signature ให้เป็นปัจจุบัน และสั่ง Full-Scan เครื่องคอมพิวเตอร์และหลังจากนั้น Restart เครื่อง



รูปที่ 4.21 Process UpdateService.exe ติดต่อมายัง NGINX (172.18.72.223)



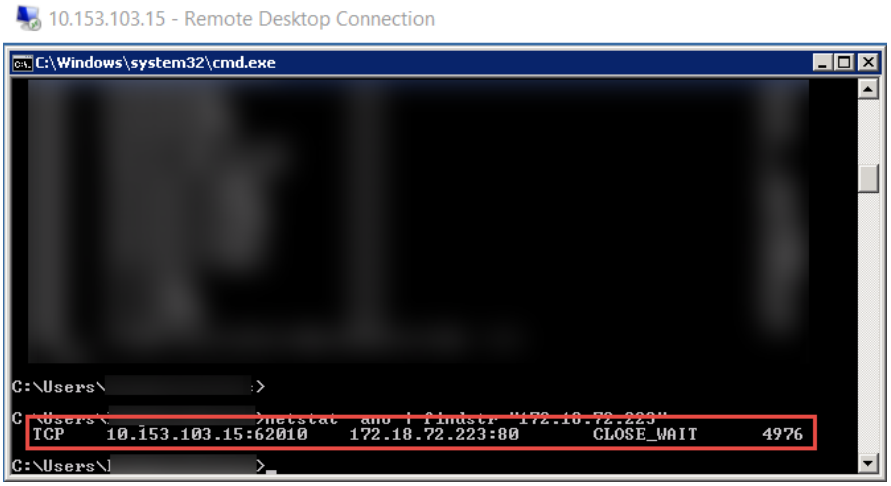
รูปที่ 4.22 ที่อยู่ของไฟล์มัลแวร์



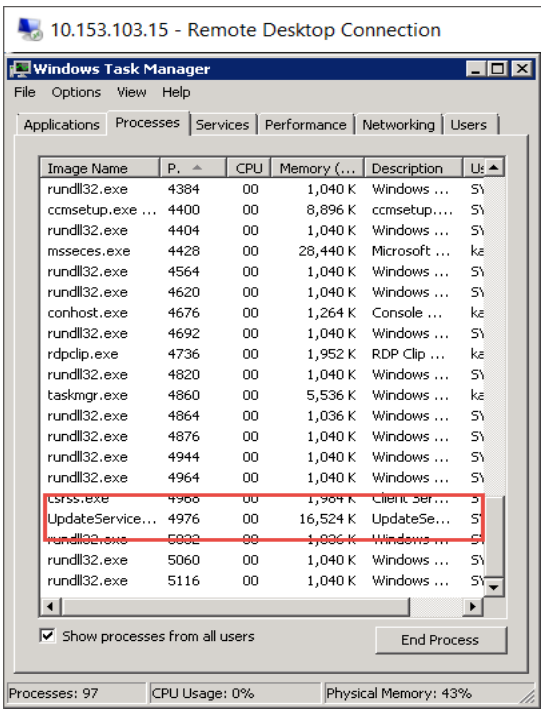
รูปที่ 4.23 Virustotal แจ้งว่าเป็นมัลแวร์

6) C&C Server : mebel-proxy.com.ua และ IP : 10.153.103.15

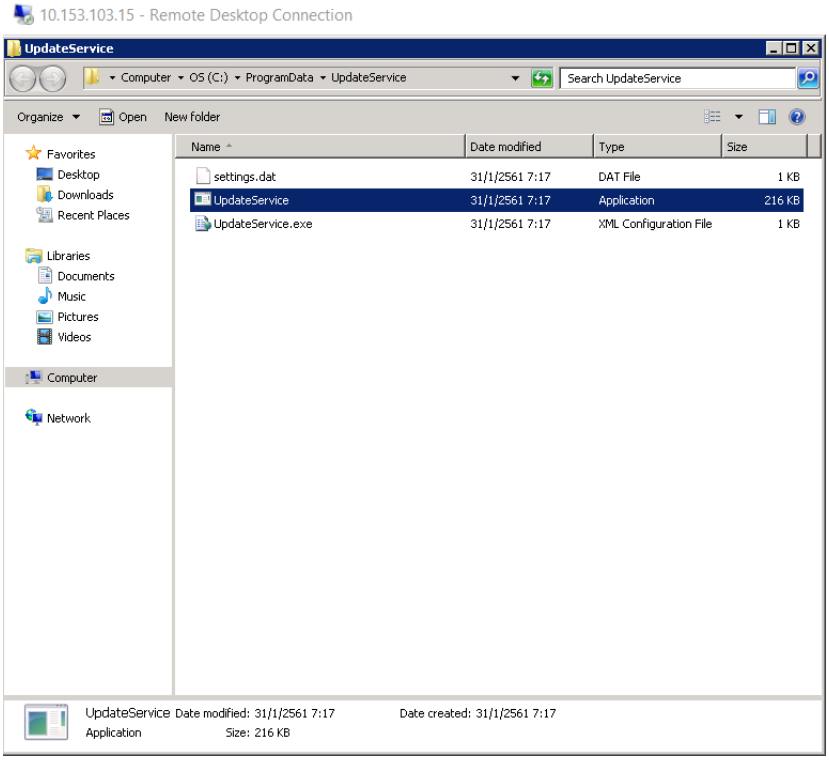
จากการสำรวจ เมื่อ Remote ไปยัง IP 10.153.103.15 พบว่า มีการเชื่อมต่อมายัง NGINX ดังรูปที่ 4.24 โดยเชื่อมต่อมาด้วย PID 4976 เมื่อตรวจสอบ PID ดังกล่าว พบ Process ที่ชื่อว่า UpdateService.exe ดังรูปที่ 4.25 เมื่อนำไฟล์ดังกล่าวไปตรวจสอบกับ Virustotal พบว่าเป็นมัลแวร์ ดังรูปที่ 4.26 และ 4.27



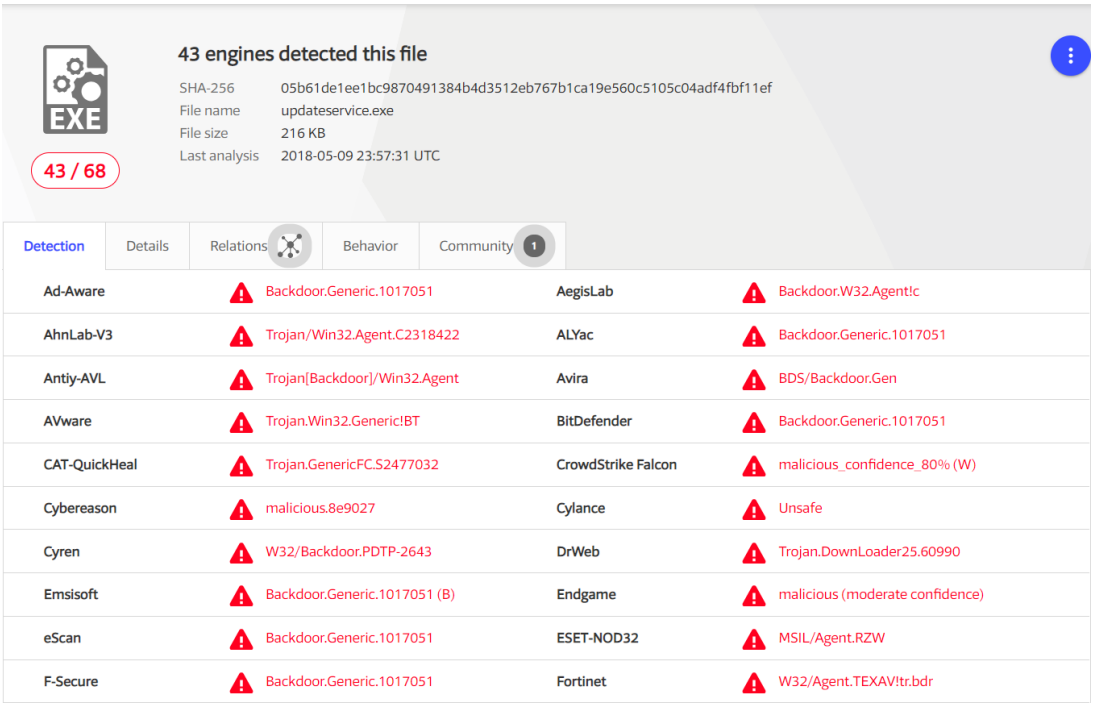
รูปที่ 4.24 PID 4976 ติดต่อมายัง NGINX (172.18.72.223)



รูปที่ 4.25 PID 4976 คือ Process UpdateService



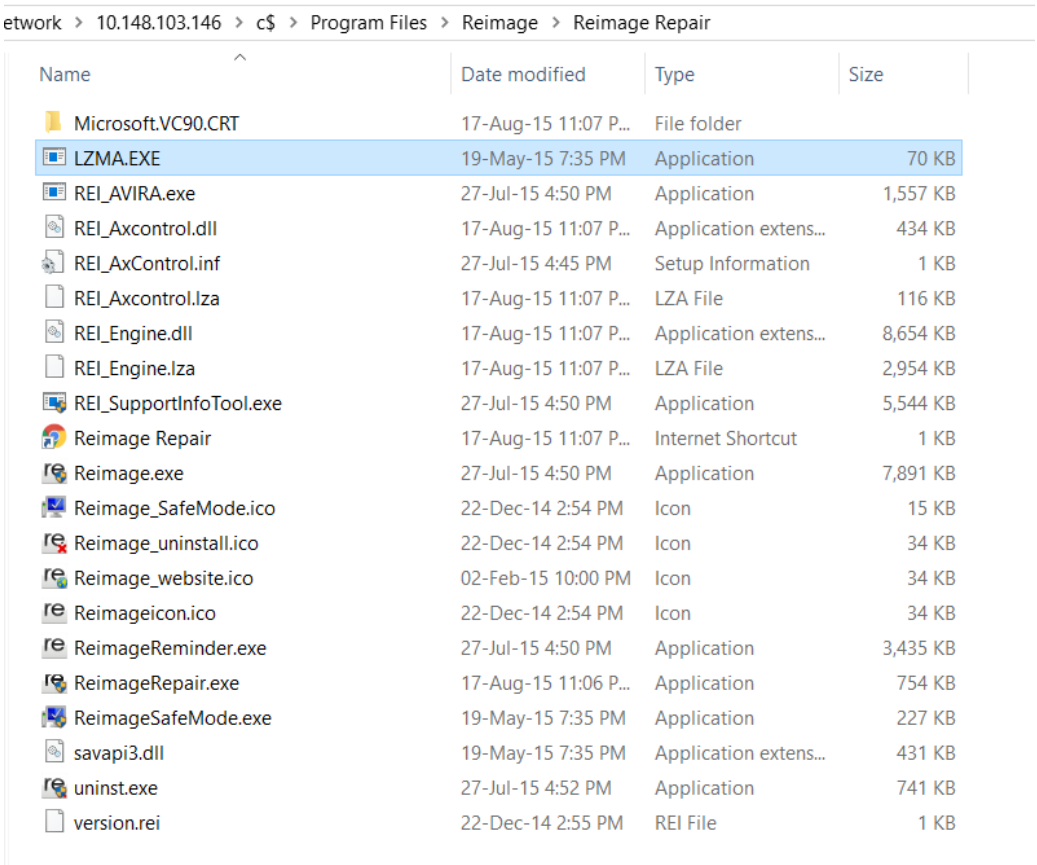
รูปที่ 4.26 ที่อยู่ของไฟล์มัลแวร์



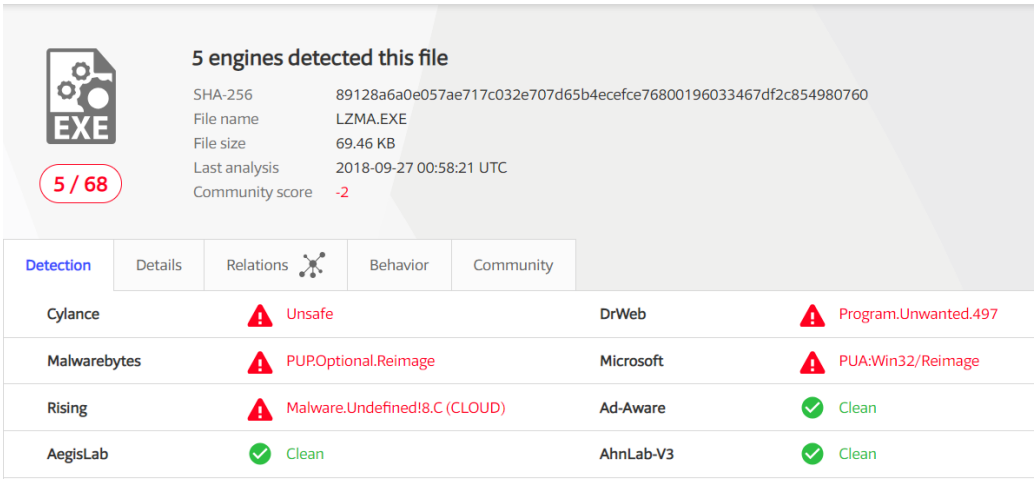
รูปที่ 4.27 Virustotal แจ้งว่าเป็นมัลแวร์

7) C&C Server : cdnrep.reimage.com และ IP : 10.148.103.146

จากการสืบค้นข้อมูลพบว่า C&C Server : cdnrep.reimage.com นั้นมีมัลแวร์ชื่อ Reimage ที่คล้ายกับ Baidu โดยที่จะบอกสรรพคุณของโปรแกรมว่า เหมือนติดตั้งแล้วจะทำให้เครื่องคอมพิวเตอร์เร็วขึ้น ซึ่งเมื่อติดตั้งโปรแกรมดังกล่าวจะส่งผลให้เครื่องคอมพิวเตอร์ช้าลง และหลอกให้จ่ายเงินซื้อโปรแกรมเพื่อทำให้เครื่องคอมพิวเตอร์เร็วขึ้น ซึ่งหากติดตั้งโปรแกรมดังกล่าว ตัวโปรแกรมจะไปอยู่ที่ C:/Progran Files/Reimage และเหมือนตรวจสอบไฟล์ LZMA.EXE Virustotal แจ้งว่าเป็นมัลแวร์ดังรูปที่ 4.28 และ 4.29 ซึ่งแก้ไขได้โดยการถอนการติดตั้งโปรแกรมดังกล่าวและ Restart เครื่อง



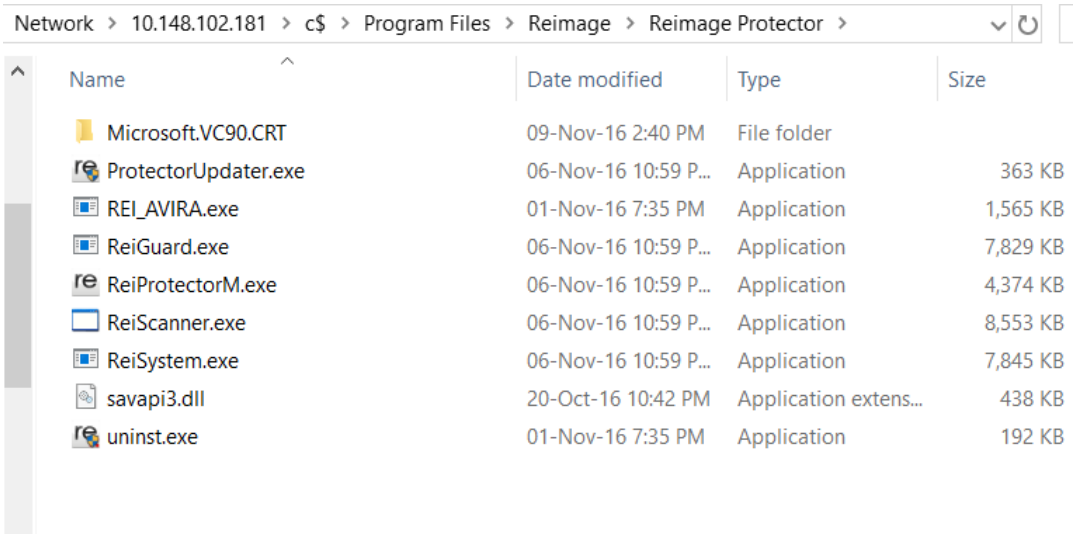
รูปที่ 4.28 ที่อยู่ของโปรแกรม Reimage



รูปที่ 4.29 Virustotal แจ้งว่าเป็นมัลแวร์

8) C&C Server : cdnrep.reimage.com และ IP : 10.148.102.181

จากการสำรวจพบว่าเครื่อง IP 10.148.102.181 มีการติดตั้ง Reimage เช่นกัน แต่ไม่ได้ติดตั้ง Reimage Repair เหมือนกับเครื่อง 10.148.103.146 แต่ก็ยังคงสรุปได้ว่าเป็นเครื่องที่ติดมัลแวร์อยู่ เพราะมีการติดตั้ง Reimage เช่นกัน ดังรูปที่ 4.30



รูปที่ 4.30 Virustotal แจ้งว่าเป็นมัลแวร์

บทที่ 5

สรุปผลการดาเนินงาน

5.1.ผลการดำเนินงาน

ผลการดำเนินงานช่วยให้ตรวจพบเครื่องที่ติดมัลแวร์ภายในองค์กรได้ครอบคลุมมากกว่าเดิม และสามารถแยกแยะได้ว่า แต่ละเครื่องมีมัลแวร์ตัวไหนทำงานอยู่ ซึ่งมัลแวร์แต่ละตัววิธีการตรวจสอบต่างกัน และมัลแวร์บางชนิด ใช้ Anti-Virus อย่างเดียวไม่สามารถแก้ไขได้ ซึ่งทำให้สามารถหาแนวทางแก้ไขได้รวดเร็วและถูกวิธียิ่งขึ้น

5.2.ปัญหาและอุปสรรค

5.2.1. จำนวนการสำรวจอาจจะมีจำนวนน้อยเกินไปหากเทียบกับจำนวนเครื่องคอมพิวเตอร์ทั้งหมดที่มีใน Report จึงทำให้ข้อมูลใน Report ส่งผลให้ยังไม่สามารถยืนยันได้ว่าจะไม่มี False Positive เลย

5.2.2. เนื่องจากการ Remote เข้าไปสำรวจอาจต้องทำเรื่องขออนุญาต Remote เข้าไป ซึ่งยังยืนยันไม่ได้ว่าเครื่องติดมัลแวร์จริง ทำให้ไม่สามารถขอ Remote แก้ไขเชิง Incident ได้

5.2.3. สำหรับการสำรวจไฟล์ในเครื่องคอมพิวเตอร์ Credential ที่มีอยู่ไม่สามารถตรวจสอบได้ทุกเครื่อง ซึ่งสามารถเข้าไปตรวจสอบได้แค่ส่วนน้อยเท่านั้น

5.2.4. C&C Server บาง Domain ถูกติดต่อด้วย Service ที่ชื่อว่า svchost ซึ่งการจะพิสูจน์ได้ว่าเครื่องติดมัลแวร์ อาจจะต้องผ่านกระบวนการ Forensic เท่านั้น การสำรวจด้วย Remote และตรวจสอบไฟล์ผ่าน Network ยังไม่ตอบโจทย์ทุก C&C Server

5.2.5. ตรวจสอบ Log ที่อุปกรณ์ Firewall พบว่าไม่ได้มีเพียงแค่ 80 กับ 443 เท่านั้น

5.2.6. ระบบ Splunk ที่ใช้เป็น License Free จึงไม่สามารถส่ง Email ได้

5.3. แนวทางการพัฒนา

5.3.1. เพิ่มจำนวนในการสำรวจเพื่อเพิ่มความมั่นใจว่า ระบบจะไม่เกิด False Positive

5.3.2. ตรวจสอบ Port อื่นๆเพิ่มเติม เพื่อลดการเกิด False Negative ของระบบ

5.3.3. จัดทำคู่มือการสำรวจและวิธีการแก้ไขในแต่ละมัลแวร์แต่ละตัว

5.3.4. ส่ง Log เข้าสู่ระบบ SIEM ที่หน่วยงานใช่อยู่เพื่อใช้ในการ Monitor เพิ่มเติม

เอกสารอ้างอิง

[1] Wikipedia, มัลแวร์, 23 ธันวาคม 2561, [Online]. Available: https://th.wikipedia.org/wiki/มัลแวร์

[2] US-CERT, Alert (TA18-201A) Emotet Malware, [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-201A

[3] IceSuntisukt, DNS (Domain name system), [Online]. Available: https://icesuntisuk.blogspot.com/2016/04/dns-domain-name-system.html

[4] นายสุไรนันท์ ขะมิมะ, Next Generation Firewall, [Online]. Available: https://www.gotoknow.org/posts/481771

[5] Mr. Apiwat Tatsanakitti, หลักการทำงานของ Proxy Server และ Reverse Proxy [ฉบับละเอียดอ่อน], [Online]. Available: http://network99public.blogspot.com/2016/06/proxy-server-reverse-proxy.html

[6] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), Security Information Manager, [Online]. Available: https://www.thaicert.or.th/papers/technical/2013/pa2013te008.html

[7] Techtalkthai, Cisco Umbrella, [Online]. Available: https://www.techtalkthai.com/cisco-announces-umbrella-secure-internet-gateway-on-cloud-solution/