บทความวิจัย

การประชุมวิชาการวิศวกรรมศาสตร์และเทคโนโลยี มทร.พระนคร ครั้งที่ 3

Proceedings of the 3rd RMUTP Conference of Engineering and Technology

การศึกษากระบวนการทำงานของ Mirai Botnet ในความปลอดภัยด้านไซเบอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

The Mirai Botnet Work Process Study Cybersecurity of Rajamangala University of Technology Phra Nakhon

นิลมิต นิลาศ[1]

[1]สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

1381 ถนนประชาราษฎร์ 1 แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพมหานคร E-mail: nilamit.n@rmutp.ac.th

บทคัดย่อ

การศึกษากระบวนการทำงานโปรแกรม Mirai Botnet ซึ่งเกิดผลกระทบลูกค้าของระบบการสื่อสารของประเทศในยุโรป ทำให้ผู้ใช้งานนับแสนรายไม่สามารถใช้งานอินเทอร์เน็ตได้ทำให้ Bandwidth ถูกใช้เกือบถึง 1 TB/s และเกิดผลกระทบการโจมตีทั่วโลกแบบ DDoS เนื่องจากเครือข่ายของมหาวิทยาลัยฯเชื่อมโยงอินเทอร์เน็ตจึงมีผลกระทบได้ จากการศึกษาพบว่าการทำงานของโปรแกรม Mirai นั้นเน้นการเกิดกับอุปกรณ์ IoT โดยเฉพาะกล้องในระบบเครือข่ายในชิปกลุ่ม ARM ARM7 Motolora 6800 PowerPC SPC x86 SuperH (SH4) จำกัดใช้เฉพาะกับ IPV4 โดยมีไฟล์ 16 ชุดมีฟังก์ชันโดยรวม 138 ฟังก์ชันรวมแล้วโปรแกรมมีมากกว่า 5,500 บรรทัดประกอบด้วยภาษา Golang และ C โจมตีแบบ Flood แบบต่าง ๆ ประมาณ 9 แบบ ผ่านพอร์ท 22, 23, และ 80 ในโปรแกรมมีการยกเว้นการเข้าถึงหน่วยงานรัฐ DoD IANA และหน่วยงานเอกชน GE HP ข้อเสนอแนะการใช้อุปกรณ์ต่าง ๆ รวมทั้งกล้องบนอินเทอร์เน็ตควรปิดการ Telnet และพอร์ท 22, 23, และ 80 หรือใช้วิธีการอื่นที่เหมาะสมป้องกันการทำให้เกิด Flood บนระบบป้องกัน APT รวมถึงการสร้างชื่อผู้ใช้งานและรหัสผ่านที่ซับซ้อน

คำสำคัญ: มิราอิ, บอทเน็ต, เมลแวร์, ดีดีโอเอส, ความปลอดภัยบน ไอโอที

Abstract

This study of the impact of Mirai botnet process to the network firms and the Internet clients around the world such as in Germany effected more than 90,000 people they cannot used the Internet because of nearly 1 TB/s bandwidth used by Mirai effectiveness. The Mirai DDoS made huge effectively gain. However, the university networking connected to Internet. From the source code the author found the Mirai program targets to IoT devices. Especially, the network cameras based-on ARM, ARM7, Motorola 6800, PowerPC, SPC, x86, and SuperH with IPV4, none of IPV6, 16 set of files with 138 functions more than 5,500 lines of code. The development languages consisted of Go and C languages for building flood in 9 different types throughout 22, 23 and 80 ports. In the code built to exceptional DoD, IANA government IPs and the big commercial firms i.e. GE and HP companies. The author recommends all network devices should closed telnet 22, 23, 80 ports, may be usage suitable protection from network flood on the APT protection included good user account names and complicated passwords.

Keywords: Mirai, Botnet, DDoS, Malware, IoT security

1. บทนำ

เนื่องจากปัจจุบันการเผชิญกับ Malware[1] ชนิดต่าง ๆ ในโลกอินเทอร์เน็ตนั้นพบได้ โดยทั่วไปที่เกิดขึ้นกับระบบคอมพิวเตอร์ของหลายหน่วยงาน เช่น หน่วยงานด้านการเงิน ธนาคาร บริษัท มีทั้งแบบทำให้เกิดความเสียหาย แบบที่ต้องการขโมยข้อมูลของเป้าหมาย อีกทั้งเป็นการแสดงศักยภาพของผู้เขียนหรือพัฒนา Malware[1] ขึ้นมาที่มีองค์ความรู้เป็นอย่างดีเยี่ยมในระบบ และเป็นเหตุยุ่งยากแก่การแก้ไขเมื่อระบบมีโปรแกรมเหล่านี้ฝังลงไปในเครื่อง ทั้งโดยบังเอิญของผู้ใช้งานเครื่องหรือโดยจงใจจากผู้ส่งไฟล์โปรแกรมเพื่อโจมตีซึ่งพอแยกออกได้ดังนี้

1) เพื่อหยุดการทำงานของระบบเครือข่ายคอมพิวเตอร์
2) เพื่อเข้าสู่พื้นที่เก็บข้อมูลสำคัญของหน่วยงาน
3) เพื่อสร้างความเสียหายทำให้ข้อมูลหายไปจากระบบ
4) เพื่อขโมยข้อมูลส่วนตัว ข้อมูลบริษัท หรือข้อมูลลูกค้า
5) เพื่อสร้างช่องทางกลไกในการเข้าถึงข้อมูลในอนาคต

จากรายงานของผู้เชี่ยวชาญด้านการตรวจสอบและต่อต้าน Virus Malware และ Trojan ที่เป็นที่รู้จักเป็นอย่างดีในตลาดโปรแกรมสำหรับป้องกันและช่วยในการกำจัด ได้มีรายงานต่าง ๆ เช่นจาก McAfee [1] จากปี ค.ศ. 2015 จนถึง ค.ศ. 2017 มี Malware แบบใหม่ ๆ เกิดเพิ่มขึ้น 10% และ Malware ของโทรศัพท์มือถือเพิ่มมากถึง 60% แนวโน้มที่เพิ่มของทางด้าน Symantec ที่มีรายงาน[2]

แบบที่ต้องการเรียกค่าไถ่ (Ransom) ร่วมถึงการทำสงครามบนระบบเครือข่ายอินเทอร์เน็ต (Cyberwar) ทุกในช่วงปี ค.ศ. 2016 ได้ปรากฏว่ามีผู้ส่งโปรแกรม Malware ออกสู่ระบบอินเทอร์เน็ตทำให้เกิดการใช้แบนด์วิธด์ของระบบเครือข่ายอย่างมากทำให้เกิดภาวะเครือข่ายไม่สามารถใช้งานปกติได้เป็นที่รู้จักในนาม Mirai มาจากการ์ตูนญี่ปุ่น 未来日記 Mirai Nikki[3] ในเอกสารนี้ขอใช้คำทับศัพท์ภาษาอังกฤษ Mirai มาจากภาษาญี่ปุ่น 未来 หมายถึง “อนาคต” หรืออีกทั้งเป็นชื่อรุ่นรถยนต์หรือชื่อคนเป็นต้น เพื่อทำให้ผู้คนสับสนจากแหล่งที่มา

รูปที่ 1 The Future Diary หรือ Mirai Nikki[3]

โดยระบบที่ถูกพัฒนาขึ้นนี้มีศักยภาพสูงมากในการก่อให้เกิดผลรุนแรงและอย่างใหญ่หลวงกับระบบเครือข่ายทั่วโลก ทำให้เป็นที่กล่าวขานถึง ผู้วิจัยให้ความสำคัญกับ Malware ชนิดนี้ซึ่งเป็นแบบ DDoS (Distribute Denial of Service)[4-6] แบบหนึ่งที่มุ่งโจมตีอุปกรณ์จำพวกกล้องอินเทอร์เน็ตที่เรียกว่า IP Camera และสามารถทำให้สร้างเครือข่ายของ Botnet ที่มีขนาดใหญ่มากทำให้เกิดผลกระทบอย่างกว้างขวาง ที่เรียกว่าการโจมตี Cyber Attack ที่มีอย่างต่อเนื่องเพื่อให้บรรลุเป้าของระบบเครือข่ายที่ไม่สามารถใช้การได้ รวมถึงอาชญากรรมไซเบอร์ที่เรียกว่า Cybercrime ดังนั้นการศึกษาโปรแกรมของ Mirai Botnet[5] จึงมีความจำเป็นที่ต้องศึกษาและทำความเข้าใจเพื่อรับมือ โดยเทียบเคียงกับโมเดลมาตรฐานของ DDoS เพื่อทำความเข้าใจถึงศักยภาพการทำงานของโปรแกรม

2. หลักการทำงานและโปรแกรม

2.1 การทำงานแบบ Botnet

ระบบการทำงานของ Botnet นั้นมีหลายส่วนแต่โดยรวมมีส่วนที่สำคัญและต้องกล่าวถึงประกอบด้วยสามส่วนหลักได้แก่ ส่วนของตัว Bot หรือ Botnet ทำหน้าที่ในการกระจ่ายหรือเก็บรวบรวมข้อมูลของเครื่องเป้าหมายส่วนของตัว Loader เพื่อทำการโหลด Bot ไปสู่เครื่องเป้าหมายในการโหลด Bot เมื่อโหลดเข้าเครื่องเป้าหมายแล้วต้องสามารถทำงานได้ Execute โปรแกรม Bot ได้และส่วนที่สำคัญอีกอย่างคือส่วนของการควบคุม Command and Control ที่เรียกโดยย่อว่า CnC หรือ C2 ที่จะทำหน้าที่รับคำสั่งจาก Hacker หรือผู้ส่งเพื่อควบคุมการทำงาน การกระตุ้นให้เกิดการทำงานของโนดที่ติด Malware ว่าให้โนดใดทำงานบ้างแต่ทั้งนี้ต้องอยู่บนระบบเครือข่ายที่สมบูรณ์

1) Bot

2) Loader

3) Command and Control หรือ CnC

รวมถึงองค์ประกอบโปรแกรม Script ในการสร้างฐานข้อมูลเพื่อเก็บของมูลของโนด ระหว่างทางและโนดเป้าหมาย ที่มีโครงสร้างในแบบที่เรียกว่าเป็น Denial of Service (DoS) ซึ่งมีเป้าหมายต่อเครื่องคอมพิวเตอร์ในระบบเครือข่ายชัดเจนในการปฏิบัติการ

2.2 โปรแกรม DDoS และการวิเคราะห์

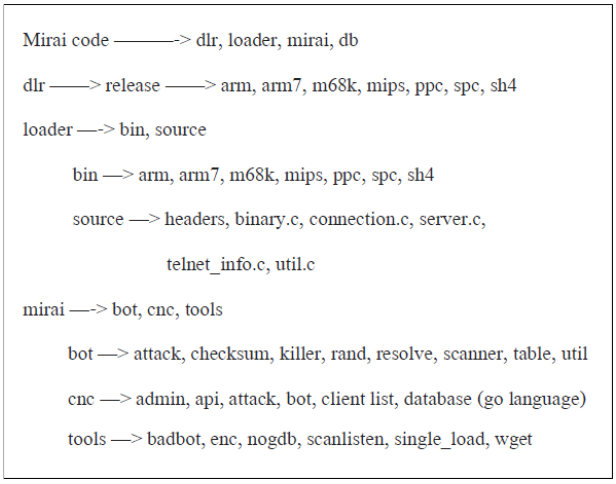
กระบวนการศึกษาและวิเคราะห์ Botnet มีสองประเภทคือการศึกษาแบบพลวัต (Dynamic) กับการศึกษาแบบสถิต (Static) ในงานนี้เนื่องจากมี Source code จึงสะดวกในการเรียนรู้โครงสร้างของภาษาที่ใช้พัฒนาอย่างสะดวก เพราะโดยกระบวนการแล้วต้องนำไฟล์ทำงานนั้นมาทำวิศวกรรมย้อนรอย (Reverse engineering) เพื่อให้ได้โค้ดภาษาแอสเซมบลี่ออกมาแล้วจึงทำการแปลงให้เป็นภาษาระดับสูงอื่น ๆ ตามแต่ผู้ออกแบบและผู้พัฒนาขึ้นได้ใช้เครื่องมือพัฒนาโปรแกรมแบบใด

2.3 องค์ประกอบของโปรแกรม

ผู้พัฒนาโปรแกรมได้ใช้ภาษาหลักอยู่สองภาษาคือภาษาซี ด้วยตัวแปรภาษา gcc และภาษาโก Golang จากซอร์สโค้ดถูกออกแบบไว้เป็นสี่ส่วนหลัก ๆ คือ dlr loader mirai database[5] มีรายละเอียดของแต่ละส่วนต่อไปนี้

ส่วนของ dlr เป็นส่วนในการส่งโค้ดไปยังอุปกรณ์เป้าหมายซึ่งขึ้นกับตัวประมวลผลหลักของเป้าหมายได้แก่ ARM ARM7 M68K MIPS PPC SPC SH4 x86 ซึ่งเป็นตัวประมวลผลส่วนมากที่กล้องบนระบบเครือข่ายใช้งานกันอย่างแพร่หลายในตลาดและเครื่องคอมพิวเตอร์ที่ใช้กันทั่วไป

ส่วนของ loader ประกอบด้วยสองส่วนคือ bin และ source ที่แยกเก็บโปรแกรมระหว่างชุดที่ใช้ในกล้องบนเครือข่ายอินเทอร์เน็ต และส่วนของโปรแกรมภาษาซีที่ใช้ในการเชื่อมต่อและเข้าถึงเซิร์ฟเวอร์ ดังในรูปที่ 2 ส่วนของ header นั้นมีการพัฒนาโปรแกรมเพิ่มเติมขึ้นเป็น header files ที่ถูกเรียกใช้งานจากโปรแกรมย่อยต่าง ๆ โดยในส่วน mirai แบ่งองค์ประกอบสามส่วนคือ bot cnc และ tools โดยมีไฟล์ภายในครบองค์ประกอบในการทำงานอย่างพร้อมเพียง ทำให้น่าศึกษาวิธีการพัฒนาและการเรียนรู้เพื่อหาแนวทางในอนาคตที่มีแนวโน้มในการพัฒนาโปรแกรมให้ศักยภาพยิ่งกว่าที่เป็นอยู่อีก



รูปที่ 2 โครงสร้างองค์ประกอบของโปรแกรม Mirai [5]

พัฒนาและการเรียนรู้เพื่อหาแนวทางในอนาคตที่มีแนวโน้มในการพัฒนาโปรแกรมให้ศักยภาพยิ่งกว่าที่เป็นอยู่อีก

2.4 ส่วนประกอบในการโจมตี

โปรแกรมมีหลายส่วนในที่นี้ขอแสดงเฉพาะบางส่วนเพื่อให้ทราบถึงการพัฒนาโปรแกรม Mirai [5]

"include.h", "attack.h", "rand.h", "util.h", "scanner.h"

attack_udp_generic, attack_udp_vse, attack_udp_dns, attck_udp_plain

attack_tcp_syn, attack_tcp_ack, attack_tcp_stomp

attack_gre_ip, attack_gre_eth

attack_app_proxy, attack_app_http

เมื่อโจมตีใน Mirai ใช้โปรแกรมภาษาโก (Go) เป็นส่วนที่อยู่ใน CnC [5] เพื่อทำการโจมตี โดยมีการใช้ attackInforLookup ดังนี้

"udp" : UDP flood,

"vse": Valve source engine specific flood,

"dns": DNS resolver flood,

"syn": SYN flood,

"ack" ACK flood,

"stomp": TCP stomp flood,

"greip": GRE IP flood,

"greeth": GRE Ethernet flood,

"udpplain": UDP flood,

"http": HTTP flood

สามารถสร้าง Floods แบบต่าง ๆ ได้ถึง 10 อย่าง นับว่ามีศักยภาพยิ่ง

2.6 ข้อมูลทั่วไปจากภายในโปรแกรม

โปรแกรมที่เขียนส่วนใหญ่พัฒนาขึ้นด้วยภาษาซี และมีการเขียนโค้ดของชื่อผู้ใช้ในระบบและรหัสผ่าน โดยชื่อ root มี 20% admin 9% อื่น ๆ ในตารางที่ 1 หมายถึงการใช้ชื่อที่แตกต่างและชื่อที่เป็นคำหยาบ ส่วนอื่น ๆ ในตารางที่ 2 เป็นคำหยาบ

ในการใช้ตัวแปรของโค้ดภาษาซีมีการใช้ Pointer ช่วยในการอ้างถึงข้อมูลในหลายฟังก์ชันและใช้ใน structure ไปถึงการใช้เทคนิค Pointer ซ้อน Pointer รวมถึงการใช้ ifdef--endif ในหลายช่วงของโปรแกรมฟังก์ชัน main() และฟังก์ชันอื่น ๆ บางส่วนที่น่าสนใจดังตัวอย่างโปรแกรม

```
#ifdef MIRAI_TELNET //from the attack_killer_all function
    scanner_init();
#endif
struct attack_target *targs = NULL; //from the attack_parse function
volatile int running_threads = 0;
volatile unsigned long found_srvs = 0; //use volatile quantifier
```

การใช้ volatile เพื่อช่วยกับตัวแปรในโปรแกรมทำให้เห็นว่าผู้พัฒนามีความเชี่ยวชาญและใช้ประโยชน์สูงสุดจากคำสั่งในภาษาโปรแกรมมิ่ง จากตารางที่ 1 ชื่อผู้ใช้งานในโปรแกรมต้นฉบับมีซ้ำกันโดยเฉพาะชื่อ root และ admin มีรวมแล้ว 46 ชื่อซึ่งมากกว่ากึ่งหนึ่งของรายชื่อในโค้ดต้นฉบับ ส่วนรหัสผ่านในตารางที่ 2 นั้นเป็นตัวอักษรอย่างเดียวมากสุดในรายชื่อส่วนตัวเลขอย่างเดียวในลำดับรองลงมารวมแล้วมากกว่ากึ่งหนึ่งของรายชื่อในไฟล์ต้นฉบับ

ตารางที่ 1 ข้อมูลของชื่อผู้ใช้และจำนวนที่ปรากฏในโค้ด

Account Name	Number
root	32
admin	14
guest	3
Administrator	1
Others	12

จากตารางที่ 1 เห็นได้ว่าการตั้งชื่อผู้ใช้งานบนระบบหรือบนอุปกรณ์กล้องมีความละหลวมอีกทั้งรหัสผ่านก็เป็นเพียงตัวเลขธรรมดาที่ 12.4% หรือตัวอักษรธรรมดาที่สามารถคาดเดาได้ง่าย 18.6% การผสมระหว่างตัวเลขและตัวอักษรมีเพียง 9 รายการคิดเป็น 5.31% ของรหัสผ่านที่เป็นตัวเลขอย่างเดียวกับตัวอักษรอย่างเดียว โดยไม่มีอักขระพิเศษเลยซึ่งจากตัวโค้ดได้คัดกรองออกมาได้ตามตารางที่ 2 เห็นได้ว่าควรเป็นอย่างยิ่งในการใส่รหัสผ่านด้วยอักขระพิเศษเพื่อทำให้เกิดการหน่วงเวลาการเข้าถึงและควรมีการปรับเปลี่ยนรหัสผ่านทุกช่วงเวลาที่ไม่นานเกินในการใช้งานโดยสร้างเป็นเสมือนข้อบังคับของหน่วยงานให้บริการ

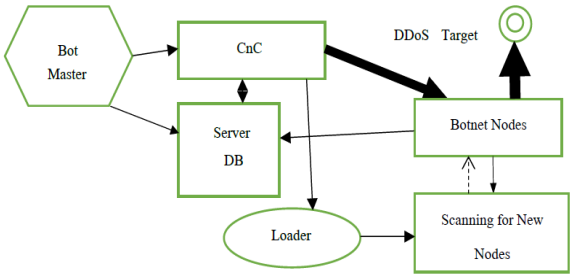
ตารางที่ 2 ข้อมูลรหัสผ่านที่แยกตามกลุ่มของตัวเลข ตัวอักษรและอื่น ๆ

รหัสผ่าน	จำนวนที่ปรากฏในโค้ด
ตัวเลข	20
ตัวอักษร	30
ตัวเลขผสมตัวอักษร	9
none	2
อื่น ๆ	1
สัญลักษณ์พิเศษ*	-

*สัญลักษณ์พิเศษในภาษาอังกฤษเช่น @ ! $ % & ~ เป็นต้น

2.8 ผังการทำงาน

จากที่ได้ศึกษาเรียนรู้จากโปรแกรมต้นฉบับทำให้สามารถร่างผังการทำงานของระบบโดยรวมดังรูปที่ 3 ที่การส่งคำสั่งจาก CnC นั้นไปถึงยังโนดจำนวนมากแต่ละอันที่ได้ติดตั้งโปรแกรมพร้อมรับคำสั่งและส่งข้อมูลโจมตีจากแต่ละโนดจำนวนมากพร้อมกัน เกิดภาวะทำให้เครื่องเป้าหมายของการโจมตีไม่สามารถรับมือได้ ทำให้ระบบเครื่องไม่ตอบสนอง โดยตัวเซิร์ฟเวอร์ที่จัดเก็บข้อมูลใช้ใน Mirai เป็น MySQL



รูปที่ 3 ผังการทำงานขององค์ประกอบแต่ละส่วนของ Mirai

3. สรุป

จากการศึกษานี้ทำให้ทราบข้อมูลที่เป็นประโยชน์ในหลายด้าน โดยเฉพาะการตั้งชื่อผู้ใช้งานบนระบบและรหัสผ่านที่ผู้ให้บริการละหลวมในทางปฏิบัติเช่นตัวเลขที่คาดเดาได้ง่าย ชื่อที่คาดเดาได้ง่าย อีกทั้งใช้รหัสผ่านที่ไม่มีอักขระพิเศษทำให้ง่ายต่อการเข้าถึงเพื่อเข้าสู่ระบบและฝังโค้ดของ Mirai Botnet และส่งด้วยโปรโตคอล TCP UDP HTTP เข้าสู่ระบบอินเทอร์เน็ตพร้อมเพรียงกันทำให้ใช้ Bandwidth อย่างมากขึ้นด้วยการทำให้เกิด flood กว่า 9 แบบที่ขึ้นกับองค์ประกอบเครื่องหรือกล้องบนระบบอินเทอร์เน็ตบนโปรแกรมมากกว่า 5,500 บรรทัด 138 ฟังก์ชันบนชิป 6 ตระกูลที่นิยมใช้งานในกล้องบนระบบเครือข่ายอินเทอร์เน็ต

การเพิ่มความระมัดระวังเป็นสิ่งที่ทำให้ผู้ใช้งานหรือโดยเฉพาะในกลุ่มงานที่ต้องรับผิดชอบดูแลระบบเข้าถึงระบบได้ยากขึ้นแต่ก็เป็นความรับผิดชอบของผู้ให้บริการต่อผู้รับบริการที่ต้องให้บริการที่ปลอดภัยต่อการแทรกแซงจากการทำงาน DDoS บนระบบเครือข่ายอินเทอร์เน็ตด้วยการใช้งานระบบป้องกัน APT การศึกษาถึงเทคนิควิธีการใหม่ ๆ ทาง Computer Intelligence ที่อาจถูกนำมาใช้ในโปรแกรมกลุ่ม DDoS มีความสำคัญอย่างยิ่งในโลกปัจจุบัน

4. กิตติกรรมประกาศ

ขอบคุณมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร คณะวิศวกรรมศาสตร์ สวพ. และ สวส. ผู้ให้การสนับสนุนเครื่องมือและทุนวิจัยในปี พ.ศ. 2560

เอกสารอ้างอิง

[1] McAfee Labs Threat Report, December 2017

[2] Symantec, Internet Security Threat Report, Vol.22, April 2017.

[3] Sakae Esuno, “Mirai Nikki” wikipedia.org. (4 April 2017)
masenal, “Mirai Nikki”,
https://www.youtube.com/watch?v=d9MgmwtKDJ0,
Published on Nov 17, 2015. (14 March 2017)

[4] jgamblin/Mirai-Source-Code https://github.com/jgamblin/Mirai-Source-Code.git. (15 January 2017)

[5] Jelena Mirkovic, Peter Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communications Review, Vol.34, No.2, April 2004.

[6] Ian Sommerville , *Software Engineering 9th Edition*. Addison-Wesley, Pearson Education Inc., 2011.