MOMMA THE C2 FRAMEWROK

การศึกษาโครงสร้างและการทำงานของ Command and Control (C2) Framework

รายวิชา CP422 031 : Introduction to Cybersecurity

อาจารย์ที่ปรึกษา ศ.ดร.จักรชัย โสอินทร์ อาจารย์ที่ปรึกษา อ.ดร.ชาติชาย ปุณริบูรณ์

อาจารย์ที่ปรึกษา ผศ.ดร.สาธิต กระเวนกิจ

หลักการและเหตุผล

- ภัยคุกคามทางไซเบอร์ในปัจจุบันมีความซับซ้อนมากขึ้น
- ผู้โจมตีมักใช้ Command and Control (C2) เพื่อควบคุมเครื่องที่ติดมัลแวร์จากระยะไกล
- C2 เป็นโครงสร้างพื้นฐานของมัลแวร์หลายประเภท เช่น
  - RAT
  - Botnet
  - Spyware
- โครงงานนี้จึงศึกษาการทำงานของC2 Framework เพื่อทำความเข้าใจสถาปัตยกรรมของระบบ C2

ผลการศึกษาสามารถนำไปใช้วิเคราะห์ภัยคุกคามและพัฒนาแนวทางป้องกันในมุมมอง Blue Team / SOC

วัตถุประสงค์

- เพื่อศึกษาโครงสร้างและหลักการทำงานของ Command and Control (C2) Framework
- เพื่อศึกษาพฤติกรรมการสื่อสารระหว่างC2 Server และ Agent เช่น Beaconingและ Command Execution
- เพื่อวิเคราะห์พฤติกรรมที่เกี่ยวข้องกับการโจมตี เช่น
  - Data Exfiltration
  - Credential Access
  - Persistence
- เพื่อเชื่อมโยงพฤติกรรมของระบบกับ MITRE ATT&CK Framework
- เพื่อสกัดบทเรียนเชิงป้องกันสำหรับ Blue Team และ SOC

กระบวนการทำงาน

- ขั้นตอนการทำงานของระบบ
- Agent เริ่มต้นการทำงานบนเครื่อง Client
- Agent ติดต่อไปยัง C2 Server ตามเวลาที่กำหนด (Beaconing)
- C2 Server ตรวจสอบคำสั่งใหม่
- ผู้ควบคุมส่งคำสั่งผ่าน Client
- Server ส่งคำสั่งไปยัง Agent
- Agent ดำเนินการตามคำสั่ง
- Agent ส่งผลลัพธ์กลับไปยัง Server
- Server บันทึก Log และแสดงผลผ่าน Dashboard

ขอบเขตการทำงาน

ศึกษาพฤติกรรมในช่วง Post-Exploitation Phase เช่น

- C2 Communication
- Remote Command Execution
- Credential Access
- Keylogging
- Persistence
- Data Exfiltration
- โดยทำการทดลองเฉพาะใน Lab Environment เท่านั้น

องค์ประกอบของระบบ

1. C2 Server
2. Client (Control Panel)
3. Agent / Implant

Operator – > C2 Server –> Agent

สรุปผลการทำงาน

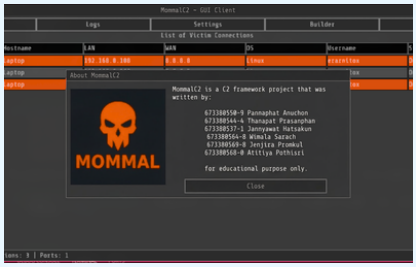
- เข้าใจสถาปัตยกรรมของ C2 Framework
- เข้าใจ Attack Lifecycle
- สามารถเชื่อมโยงกับ MITRE ATT&CK
- ช่วยพัฒนาทักษะด้าน Cybersecurity

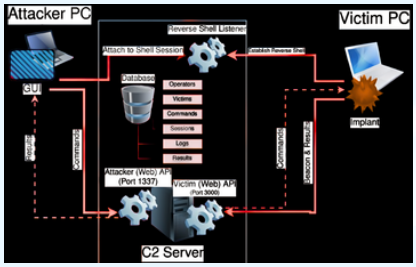
แนวทางพัฒนาในอนาคต

- เพิ่ม Windows Agent
- เพิ่ม Network Detection
- เพิ่ม Visualization Dashboard
- เพิ่ม Blue Team Detection Lab

สมาชิก group 4 sec.3

673380550-9 ปัณณพัฒน์ อนุชน
673380544-4 ธนภัทร ประสานพันธ์
673380537-1 จรรยวรรธน์ หัสคุณ
673380564-8 วิมาลา สาราช
673380569-8 เจนจิรา พรมกุล
673380568-0 อทิติยา โพธิศรี





การทำงานของระบบ

ผลลัพธ์ที่คาดหวัง

- จากการศึกษาโครงงานนี้คาดว่าจะสามารถ
- เข้าใจโครงสร้างของ C2 Framework
- วิเคราะห์พฤติกรรมของ C2 Communication
- เชื่อมโยงการโจมตีกับ MITRE ATT&CK Framework
- เข้าใจแนวทางการตรวจจับและป้องกันสำหรับ Blue Team

ภาพรวมการทำงาน

ระบบ Command and Control (C2) Framework เป็นระบบที่ใช้ควบคุมเครื่องคอมพิวเตอร์ที่ติด Agent หรือ Implant จากระยะไกลผ่าน C2 Server

ผู้ควบคุมระบบ (Operator) สามารถส่งคำสั่งไปยังเครื่องเป้าหมายผ่าน Server และรับผลลัพธ์กลับมาได้แบบเรียลไทม์

MOMMAL C2 Framework มีฟีเจอร์หลัก

- Remote Shell Management
- Credential Stealer
- Keylogger
- Beaconing over HTTPS
- Browser Impersonation
- Systemd Service Persistence
- User Interface สำหรับควบคุมระบบ

ฟีเจอร์เหล่านี้ช่วยจำลองพฤติกรรมของ C2 Framework ที่พบในมัลแวร์จริง

Architecture ของระบบ

Operator (Client UI)
|
| Command
▼
C2 Server
|
| HTTPS Beacon
▼
Agent / Implant
(Target System)

เครื่องมือและเทคโนโลยีที่ใช้

ภาษาโปรแกรม
- C++

Libraries
- Raylib / Raygui (User Interface)
- SQLiteCpp (Database)
- Glaze
- cpppwn

ระบบฐานข้อมูล
- SQLite

Network Protocol
- HTTPS

Environment
- Virtual Machine
- Cyber Range

Framework อ้างอิง
- MITRE ATT&CK Framework

COLLEGE OF COMPUTING
KHON KAEN UNIVERSITY