Threat Categorization Based on Malware’s C&C Communication

Key Words: Malware Analysis, C&C, Threat categorization , Python, Fingerprinting, pcap, Compiler, TLS

Group 6 – (KCST) Kerberos Cyber Security Team

KCST

Team Members

1. Sriram P (McAfee)
2. Mohammed Jawed (IAEA, U.N)
3. Archana Pawar (TCS)
4. Ahakam Sarosh
5. Anupama G

KCST

Synopsis

Threat categorization is one of the biggest **challenges** that the security community faces today. **Malwares** are hidden using multiple layers of **packers**, **obfuscators** thus hiding from revealing its true identity unless unpacked.

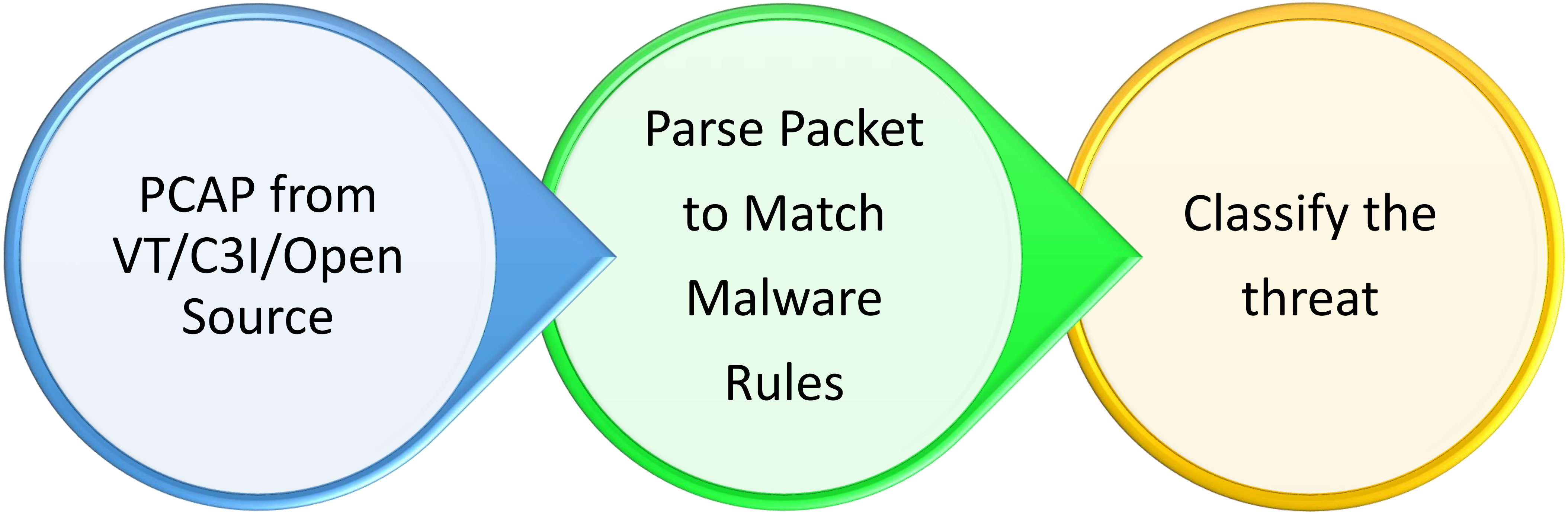
Of late, it is also observed that the same codebase / framework is reused by **multiple RAT builders** and **Backdoors**. Some of these **packers** and **obfuscators** are also reused across multiple **malware** families.

This project aims at looking into the **networking** concept of these **C&C communicating** malwares and tries to **parse** the network **packets** and try to classify the threats based on the **unique** communication pattern used by these malware families. The rules also involve **fingerprinting** the **TLS certificates** used in the communication.

Deliverables

- Python based pcap parser
- Rule and fingerprinting Compiler for pcap parser
- Usage documentation
- Complete Architect Diagram
- Demo

Diagram (OverView)



PCAP from VT/C3I/Open Source

Parse Packet to Match Malware Rules

Classify the threat

Key Words

- Malware Analysis
- Threat categorization
- C&C
- Python
- Fingerprinting
- Pcap
- Compiler
- TLS

KCST

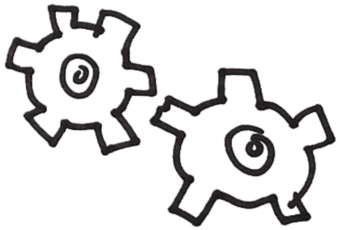
References

- https://www.youtube.com/watch?v=eEw_VZ5xdcE
- https://www.youtube.com/watch?v=NSmkrlybZXs
- https://arnon.dk/wp-content/uploads/2015/01/Malicious-traffic-detection-using-traffic-fingerprint.pdf
- https://blogs.vmware.com/security/2022/03/emotet-c2-configuration-extraction-and-analysis.html
- https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
- https://bth.diva-portal.org/smash/get/diva2:1571926/FULLTEXT01.pdf
- https://www.researchgate.net/publication/309220704_Statistical_fingerprint-based_intrusion_detection_system_SF-IDS

From IDEA

to

IMPLEMENTATION



to be continued...

KCST