Hands On Lab: Unit 7

MICS-252, Fall 2024

Threat Detection

Prepared by: Karl-Johan Westhoff

email: kjwesthoff@berkeley.edu

UC Berkleley School of Information

MICS Course 252 Fall 2024 (Kristy Westphal)

1 Introduction

In the previous Assignment unit 6 [1] the 'home network' threat model using 'STRIDE' identified the following weaknesses:

- Exploitable assets, allowing access to the network and pivot points for further exploitation
- WIFI passwords may have been leaked granting direct access to the network
- Logging is scarce, inconsistent and incoherent (Windows pc's may log a-lot, IOT devices may not log at all, logging at the NAT is limited)

2 What Are We Protecting from What?

We are protecting on our home network:

- Our login credentials (Bank, Online services etc.)
- Personal data (Documents, images etc.)
- Privacy (online activity)
- Use of your bandwidth (cost and speed)

The threats are:

- Phishing attacks to steal credentials
- Malware ('old fashioned' viruses, key loggers etc.)
- Assets being utilized as zombies in a botnet (botnets, crypto mining, etc.)
- Uncontrolled hosts on network

3 Treat Control Use Cases

Applying the:

1. Indicator
2. Data Source
3. Action

Methodology to each identified threat, gives some possible 'Use Cases'[1] for detection rules.

3.1 Phishing

Use case Outcome: Detect and block inbound phishing

- Indicators:
  - Suspicious sender
  - Suspicious domain (could be subtle changes to a URL)
  - Unusual requests e.g asking for SSN, bank account number etc.
- Data Source:
  - Email vendor/service provider phishing detection and filtering (they maintain the signatures and notifies)
  - Endpoint protection (e.g. Windows defender[2]), with an updated list of signatures
- Action:
  - Hold
  - Block/Drop (in case of known phishing sender/domain)
  - Alert

3.2 Malware

Use case Outcome: Detect malware and notify user at host level

- Indicators:
  - Endpoint protection (virus detection)
  - Unusual behavior (slowing down)
- Data Source:
  - Endpoint protection logs and notifications (EDR if equipped)
  - Network detection (NDR if equipped)
- Action:
  - Block
  - Alert

[1] I am a bit puzzled by the term 'Use Case' as it sounds like a sales argument for a SIEM, I think 'Threat Control' is a better term and can be applied holistically

3.3 DDOS zombie

Use Case Outcome: Notify network administrator (you) that botnet traffic is emerging from your public IP

- Indicators:
  - Unusual behavior (slowness, the user is the detection system here)
  - Get notified from outside[2]
- Data Source:
  - Endpoint protection (EDR if equipped)
  - Network detection (NDR if equipped)
- Action:
  - Alert
  - Block

3.4 Unwanted hosts on network

Use Case outcome: Block unauthorized hosts on network

- Indicators:
  - Unexpected host logging onto network
- Data Source:
  - NAT/DHCP server log and firewall policy
- Action:
  - Block if not on approved MAC list

4 Conclusion

Home networks are limited regarding infrastructure to detect and protect network activity and relies more on passive measures, such as subnetting and protection of individual endpoints. Home networks requirements are both simple (providing basic HTTP/S access) and complicated (providing services and protocols making things like printers simple to use). Furthermore, IOT complicates the security management, the chip sets used are cheap but still capable of doing actual computing, making them targets for use in zombie botnets. Apart from 'static' remedies such as subnetting, implementing real monitoring of the network requires some knowledge which the normal consumer does not have.
Discovering and alerting of botnets is delegated to large entities which have an overview of a network and resources to kill DDOS at a many points around the network [3].

[2] DDOS is difficult to detect, if you are part of a botnet you will likely just get the traffic going to the attacked endpoint blocked and never know about it, a mitigation may be a notification service.

Some automated firewall and network detection and response 'boxes'[4] are available to home network users with monitoring of bandwidth usage, blocking phishing, advertisement and network events. Anyway these are not 'deploy and forget' some interaction is required to interpret alerts.
Monitoring on a home networks could be allocated to the extremes of the data flow, and regard the network itself as an insecure place. Monitoring of bank transactions often happen on the bank's infrastructure, and monitoring of privacy is allocated to the endpoints on the network (things with web browsers)
Even tough the 'STRIDE' model is primarily minded for software systems, I think it actually works well for home networks with a bit of adaptation, I guess something like a home network actually resembles a system with well defined boundaries like a piece of software. The STRIDE analysis provided clear weaknesses which could then be used to define vulnerabilities for which detection mechanisms can be defined using the Indicator -> Data Source -> Action template.

References

[1] *Written Asignment 6 Threat Modelling*. `https://github.com/KJWesthoff/MICS-252-WrittenReport6/blob/21a0707597f356ef9d019f39f185c69500b531a7/WrittenAssignment6.pdf`. Accessed: 2024-10-11.

[2] *Enhanced Phishing Protection in Microsoft Defender SmartScreen*. `https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/enhanced-phishing-protection?tabs=intune`. Accessed: 2024-10-11.

[3] *Cloudflare blocks largest recorded DDoS attack peaking at 3.8Tbps*. `https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/`. Accessed: 2024-10-11.

[4] *Firewalla Commercial Producrt features*. `https://help.firewalla.com/hc/en-us/sections/115000949433-Features`. Accessed: 2024-10-11.