Theoretical Deep-Dive Into Forensics Investigation

Discussing the theoretical approach to identifying and remediating compromised systems

David C

CMP416: Digital Forensics 2

2024/25

Note that Information contained in this document is for educational purposes

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

The threat of a cyber-attack is a constant worry for any organisation, and the risk of being affected by some kind of vulnerability is only growing with 32% businesses and 24% of charities being affected by a cyber-attack throughout 2022 (Johns & Ell, 2023). As attackers are getting smarter and targeting more businesses, the techniques and capabilities of those defending these systems is improving too with digital forensics being at the forefront of those defences. Digital forensics is a process that focuses on identifying, acquiring, processing and analysing electronically stored data (Interpol, 2022). Digital forensics is crucial due to its importance with identifying the key characteristics of an attack, attributing the attack to groups known for specific things and allowing the world to improve their cyber security by sharing the necessary information to allow everyone to learn and remain safe.

This report has been written within the fictional scenario where homes are littered with Internet of Thing (IOT) devices and referred to as “smart cities”. There have been reports of one homeowner’s devices being compromised including the thermostat, security camera, TV and router. The devices have been altered in a way that appears to be intended to make the homeowner uncomfortable with the thermostat being stuck at an uncomfortable. Additionally, there is reason to believe that the network of this home is completely compromised due to changes made by the attacker to the router to show a compromise of this device.

The report that follows highlights the steps that an investigator should follow in order to successfully investigate this vulnerability and give them the best chance of not only securing the compromised devices but also provide them with relevant information to investigate and identify how an attacker may have breached the network and provide solid grounds to pursue legal ways of pursuing the attacker. Furthermore, the report highlights the OSCAR methodology and tools that are recommended for following the methodology and maximising efficiency during the investigation to reduce the stress of the individual whose home has been hacked. Finally, this report highlights the issues with the methodology highlighted throughout and things that should be considered outside of what has already been mentioned.

1.2 AIM

Throughout this report the investigator aims to highlight the steps necessary to conduct a thorough inquiry into the security weaknesses and cause of breach throughout the smart home, acquire necessary data to perform a technical analysis and then critically evaluate their findings with the intention of providing a detailed analysis to then support with the acquisition and analysis of the necessary information.

2 ACQUISITION AND INVESTIGATION STRATEGY

2.1 OVERVIEW OF METHODOLOGY

Throughout this report the investigator intends to follow the OSCAR methodology (Qureshi, et al., 2021) for highlighting the steps that would be necessary throughout this process for gaining the correct information. OSCAR highlights the importance of obtaining information, strategising the appropriate ways to collect the required information, collecting the information through the strategies previously planned, analysing the data collected and reporting and theorising on the reasons behind the attacks motivations and aims for the given scenario.

2.2 OBTAINING INFORMATION

The investigators first steps would be to obtain information regarding the incident itself, specifically when a date and time of when the event occurred, what is affected by the incident and how was it discovered. Additional information would be required regarding the legality of the situation, whether sensitive information was compromised and who the point of contact for the rest of the investigation would be as to allow the investigator to ensure they were communicating effectively with the correct person.

2.3 STRATEGISING

The strategising section of the OSCAR methodology focuses on outlining how data will be acquired as well as the general steps to ensure that the investigation go as planned. This section is of particular importance as various types of media have different volatility levels and therefore the investigator must consider a number of things when acquiring the relevant types of media.

The investigator believes that it may be beneficial to begin by mapping the network out to understand points of interest and identify areas where an attacker could have entered the network from. This could be done through the use of a network structure diagram with an example of one for this network in Appendix A – Network Structure Diagram. Following the mapping of the network, the next step of the investigators strategy process by preserving the devices present in the compromised home by accessing the systems and analysing the state of the machines and backing the machines in their current state up, into some kind of separate storage device so that they could be analysed further. Once preserved, the investigators next priority would be to run some kind of packet analysis tools such as Wireshark to monitor traffic that was going through the infected devices after the breach as this might indicate any kind of additional servers or services that the hacker was using to remain connected or have gained initial access. This could be possible using a honeypot, which is a system used to mimic a piece of infrastructure to see how devices or users may interact, whilst collecting information on what commands were being ran on the system (Kaspersky, ND). The investigator's next steps would be to

contact the system administrator of the home's systems and see if there was any kind of Network Intrusion Detection System (NIDS) in place that may have alerted them to suspicious activity, since this could further assist the investigator with later stages of their investigation.

Following a brief analysis of the information gathered above, the investigator may then head to additional homes that did not have any indicators of compromise (IoC) to setup additional logging software, both through Intrusion Detection Systems (IDS) such as Snort with specifically crafted rules for what had appeared to be abnormal data through their early analysis and Host-Based Intrusion Detection Systems (HIDS) which are more commonly used for identifying malicious activity on devices and therefore may be useful for identifying any kind of lateral movement or privilege escalation that the threat actor may be using to compromise these systems.

2.4 COLLECTION

Following the theoretical phases of this investigation, the investigator would begin collecting the information throughout this report. Following the preservation of the devices, the devices would have any logs related to either the system or network traffic retrieved, and devices checked for any known vulnerabilities using threat intelligence databases.

Furthermore, the investigators would be required to sift through the information they were collecting through these logs to ensure they were not collecting information that was redundant or not related to the situation they were investigating. An example of a tool that might be used by the investigators to do this could be Wireshark. Assuming network traffic logs were recovered, the investigators would be able to use filters to search for data from specific protocols, hosts or containing specific content.

Additionally, it would be useful to check for any kind sensors that may have been recording the data flow throughout the compromised building, either installed by the people living in the home or the security team. Sensors recording the traffic flow would often have passed this information on to external servers where they would be stored and as such, information on how traffic had passed through the firewall and around the network could be crucial for understanding how the attacker not only bypassed the security measures in place but moved laterally throughout the network compromising every smart device present.

2.5 ANALYSING

The OSCAR methodology describes the analysis phase of the methodology as the section where timelines are created, anomalies are identified and events are correlated. The investigators intended steps for conducting analysis on the information found consists of multiple focus points across the various devices.

Firstly, through the theoretical steps previously mentioned, the investigator would also aim to conduct statistical flow analysis against any network traffic retrieved from the incident. Statistical flow analysis relies on the "flow" of network traffic being recorded. A "flow" is representative of a summary of network traffic and often contains the source and destination host & port, protocol and amount of data transmitted amongst the flows. The benefit of using statistical flow analysis is that it can allow for anomalies and patterns to be identified easier due to the simplicity of the data presented. The investigator would be able to take any network captures they had been able to collect and use a tool such as Yet Another Flowmeter (YAF) which is capable of generating these flows from PCAP files and live captures, therefore providing use for it to be ran at a higher level so that it can capture traffic from additional homes and help identify anomalies in homes that were still connected to the WiFi. The investigator would recommend running this analysis tool from the offices where the security team monitored these data links.

Furthermore, an area of specific interest for the investigator could be regarding the router, as the investigator is aware that this has been compromised due to the changed Service-Set Identifier (SSID), reviewing traffic from the 802.11 protocol would be of specific importance. 802.11 is the protocol used for WiFi as the data link layer for wireless media. Management frames from the 802.11 protocol are often associated with attacks such as Evil Twin Attacks whereby an attacker creates a fake Wireless Access Point (WAP) with the same SSID as the original WAP and the devices connecting, will choose the WAP with the strongest connection and therefore could be hijacked and have encrypted data cracked or plaintext sensitive information revealed. Whilst wireless attacks should definitely be considered for the router, the investigator would also analyse the state of the router, whether there were any network rules that had been altered or changed that might allow the attacker to monitor the traffic passing through the network or pointing systems such as an administrative control panel to the open internet to allow the attacker to access the routers configuration remotely.

Alternatively, instead of the investigator relying on information that had been left over from the attack, their focus would instead shift to data that was collected whilst the breach was occurring. The investigator would aim to conduct checks on both a local and cloud level for any kind of Intrusion Prevent Systems (IPS) that may have been running and thus recorded useful information to assist with providing context or detail on the situation. An example of an IPS that may be present throughout the network could be Suricata, which is responsible for running on the devices present throughout the network and acting purely based on configured rules. Due to IPS systems operating in such a manner, it can be easy for attackers to manipulate their attacks in a way that can mask their true purpose including using alternative ports or encoding data so that when checked against the rules stored on the IPS, the attacks are not found and therefore not flagged on the machine.

2.6 REPORTING

The final stage of the OSCAR methodology highlights the importance of reporting on the information found in a coherent and factual to assist the individuals remediating the situation with a timeline of events and IOC's. A detailed and thorough report outlining the steps taken by the investigator to find the information they had found and the recommended steps for not only recovering the compromised machines but improving the overall security of the systems and potentially the wider network to best prevent against future attacks.

3 CRITICAL EVALUATION

The investigator understands that although in an ideal world the steps outlined throughout this report would be able to happen without any deterrence's or setbacks it is incredibly unlikely that this would be likely due to the complexity and potential reach of this attack. There are lots of steps in the investigators methodology that require tools or processes to have been running during the attack and configured appropriately to find the exploit or specific information required by the investigator that would correlate to the compromise of the devices in this house. To provide a ruleset that would allow IDS & IPS solutions to correctly identify the exploitation process taken by the threat actor would require a large amount of fine tuning, testing and trial & error, all of these are unlikely to have happened within the house if the user is not technically capable of doing it themselves and due to the reach of the Security Administrator, who is responsible for monitoring traffic coming through a large number of houses, is similar to searching for a needle in a haystack. Therefore, the investigators hope for the breach to have been recorded beforehand is potentially unrealistic without further information regarding the security measures in place.

Additionally, the investigator has assumed that throughout this investigation that the threat actor has not implemented any kind of defensive measures to slow down or prevent cyber security experts from being able to either recover the infected devices or information that may assist them with the identification of where or how they were compromised. There are many ways that this could be done with some examples including encryption, whereby system information could have been converted to an unreadable format and depending on the encryption, unable to be recovered without the encryption key. Alternatively, some kind of "kill switch" could have been implemented to any of the compromised system which when whatever command the kill switch had been linked to was executed, could disconnect the user, remove useful information or take the system offline completely. Both of these methods mentioned would impact the investigators proposed methodology as additional steps would need to be taken to gain access and control of the necessary information on these devices.

4 REFLECTIVE COMPONENT

The presence of a threat actor on the network whilst the investigation is underway could be catastrophic for not only the integrity of the data but also the security of the investigator and any hardware that they may connect to the compromised devices. By remaining on the network through the investigation of the compromise, the threat actor remains capable to manipulate, deceive or delete evidence that may be crucial to the investigation. Depending on the level of persistence that had been established throughout the network, the threat actor may be able to follow the investigator as they are actively performing their analysis of the compromised devices and therefore search for artefacts that may be of use for reversing the process taken to compromise the device. Alternatively, crucial components for the investigator including Operating System functionality could be altered or obscured to slow down the investigators efforts to perform their analysis

Furthermore, the investigator may be required to open or close certain ports throughout the network to be able to perform their analysis of the devices and network which could both hurt and benefit the threat actor. If the threat actor was attempting to hide the traffic they were sending and thus trying to use a port that was already open, the more open ports on the network would give provide more opportunities to hide their traffic and potentially assist them with exfiltration. Alternatively, this could also hinder the threat actors attempts to manage persistence. This could potentially be a problem for the threat actor if they had set up reverse shells or connections to internal resources through ports that were closed as part of the investigation and therefore removing some of the access established by the threat actor.

Finally, there could be a legislative element relating to the General Data Protection Regulation (GDPR) whereby sensitive information of individuals either directly or indirectly related to the occupants of the house could be at risk. If personal information such as phone numbers, email addresses or full names was associated with the devices compromised, which is likely due to the compromise of the router, then the chances of personal information being released into the hands of the threat actor is possible. This places a genuine threat to the security of those

5 DISCUSSION

5.1 CONCLUSION

Throughout this report, the investigator has aimed to concisely and clearly highlight the methodology recommended for theoretically responding, handling and mitigating the incident they had been assigned. The report highlights the importance of the OSCAR methodology and thoroughly assess the technical and non-technical aspects that should be considered through each stage of the process. The report then focuses on the specific areas that they believe would be of importance to the investigation and suggest potential attack vectors that could have been used. The report then concludes by highlighting the potential setbacks and unknown factors that the investigator is unable to account for during the acquisition phase of the investigation and the drawbacks of a situation, where the threat actor remains on the network whilst the investigation is underway.

6 REFERENCES

Interpol, 2022. *Digital Forensics.* [Online]
Available at: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics
[Accessed 9 December 2024].

Johns, E. & Ell, M., 2023. *Cyber security breaches survey 2023.* [Online]
Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
[Accessed 9 December 2024].

Kaspersky, ND. *What is a honeypot?.* [Online]
Available at: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot
[Accessed 2 December 2024].

Qureshi, S., Rajputt, F. A., Quershi, S. S. & Wajahat, A., 2021. *ResearchGate.* [Online]
Available at: https://www.researchgate.net/profile/Sirajuddin-Qureshi/publication/351998718_Network_Forensics_A_Comprehensive_Review_of_Tools_and_Techniques/links/60b4db2ba6fdcc1c66f57f65/Network-Forensics-A-Comprehensive-Review-of-Tools-and-Techniques.pdf?origin=publi
[Accessed 28 November 2024].

7 APPENDICES

7.1 APPENDIX A – NETWORK STRUCTURE DIAGRAM