Storm Investigation

Lukas Smith
Year 4 Ethical Hacking
CMP416 Advanced Digital Forensics
2022/23

Contents

Introduction 3
Scenario 3
Motivation 3
Methodology 3
Acquisition and Investigation Strategy 4
Identification 4
Preservation 5
Analysis 5
Documentation 6
Presentation 6
Discussion and Findings 7
Conclusion 9
References 10

Introduction

Scenario

The original version of the Storm botnet was linked to the Trojan horse malware 'Storm Worm' that infected users by disguising itself as a legitimate piece of software in the form of an email attachment. At its peak, the processing power Storm had available was enough 'to rival the world's top 10 supercomputers' at the time (Naraine, 2007). It was assumed that between 500,000 and 1 million computers were infected (Security Encylopedia, 2021). The botnet used a Peer-to-Peer (P2P) architecture to communicate, therefore meaning that it is decentralised and more challenging to track the controllers. Storm would also actively fight investigation, with researchers being hit with retaliation Distributed Denial-of-Service attacks against computers actively scanning a network for vulnerabilities.

Storm has now returned and infects new devices through the local network. It is known to target the latest versions of Windows and infect PCs and Android smartphones.

Motivation

The following report, written in response to a request from Microsoft London for an independent consultation on the new variant of the botnet Storm, will outline how a forensic investigation would be undertaken against said botnet. With this report, Microsoft London should be able to decide the suitability of a full forensic investigation. Additionally, this report will outline potential remediations Microsoft London can take to defend itself against similar attacks.

Methodology

The digital forensics methodology is split into five stages, the first being the most critical for this investigation.

- Identification
    - Where appropriate, data sources are identified and investigated for potential evidence.
- Preservation
    - Data is isolated and secured to ensure it is not tampered with during the rest of the investigation.
- Analysis
    - Once identified and preserved, data fragments are reconstructed, and conclusions begin to be formed.
- Documentation
    - Recording all of the evidence in order to recreate the original crime scene and determine how the breach occurred.
- Presentation
    - The investigation is summarised at a lower level to ensure all technical aspects are fully understood and that the relevant staff are informed on what to do next.

Acquisition and Investigation Strategy

Identification

The first stage of the investigation involves identifying the botnet and its sources. As the new variant of the Storm botnet infects devices through the local network, the network's physical layer can be monitored through applications such as Wireshark to identify botnet activity. If a graphical user interface cannot be used, an alternative tool is Tcpdump - a command-line-based tool. The original storm botnet used encrypted keys to identify infected machines and receive commands (Holz, et al., 2008). The keys can be found through network monitoring if this exact process is used in the new botnet. These keys can then be used to determine how many devices on the network are infected. Once the communication from the botnet has been identified, it can be used to compare against other packets or data streams to determine other communication.

Snort is another application that can be used to identify the botnet. Snort is a powerful open-source tool called an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). An IPS takes a series of rules that describe malicious network activity and identifies packets that match this type of activity. Alerts are generated based on this suspicious activity, making it easier for the investigator to narrow down the issue. Suppose Microsoft London already has an IDS. In that case, their IDS will be updated to include rules relevant to Storm, and previous alerts will be analysed for any evidence pertaining to Storm.

Additionally, the network layer should be investigated for any logs about the botnet; however, as these devices typically have a limited storage capacity, the logs they store may need to be sent to a server for analysis. This information can help identify compromised packets and their source. Furthermore, nearing the end of the investigation, this information will help reconstruct how the botnet has infiltrated the network.

In the original Storm botnet, once it infected a machine, it would disable the Windows firewall and open several TCP and UDP ports. Open ports can be checked by running the 'netstat -ab' or 'netstat -aon' command on the machine. As these ports have been opened, it is easier to narrow down possible infected devices as they can be checked to see if any unnecessary ports are open. Moreover, the firewall's state can also be examined to advise if the device is infected. (Scanlon, 2013) The firewall's state can be determined using the 'netsh' command.

The new variant of Storm also infects Android devices. As such, if Microsoft London gives employees Android-based work phones, they must be investigated further and taken to prevent the botnet from spreading elsewhere. There are several ways to extract data from mobile phones, such as Logical Extraction, where an investigator connects the device to a forensic workstation that sends several commands to the mobile device. These commands return the required data for further analysis. A potential tool for this would be LiMe, a Loadable Kernel Module (LKM) memory extractor that captures the device's volatile memory with minimal interaction, ensuring that the data retrieved is forensically sound. LiMe also provides a hash of the dumped memory, which is essential for the preservation stage.

If Microsoft London makes use of cloud services, this could create a problem during the investigation stage as these services are often hosted in locations different to Microsoft London's offices. Additionally, these services are often decentralised, meaning that data could be stored across several machines (this is to improve the reliability and the availability of data stored), which makes it harder to perform forensics on these machines.

Once the network has been initially investigated, data sources have been identified and examined, and individual devices have been assessed, the preservation stage can begin. The preservation stage happens as materials are discovered in the investigation stage to ensure no data is lost or tampered with during this stage. Meaning these two stages occur synchronously.

Preservation

Once the information has been gathered, it is imperative that it is preserved to ensure its integrity. In the event that the devices or logs are tampered with, it is essential that there is still an original copy. Compromised devices should be imaged, and all investigative work should be done on the duplicate image. Cryptographic hash values should be taken from the essential files and logs to ensure they have not been altered. Even if a singular byte is changed, the cryptographic has will change, meaning it can be proved that the document has been unaltered (Ibrahim & Jantan, 2011). If a file has been altered, it can make it inadmissible in Court. All files should also be backed up in case there is a data loss of some sort.

Once copies have been made, the original devices must be digitally isolated to preserve their meta-data. Any physical devices taken for further examination (routers, switches etc.) should be photographed to ensure their physical condition is documented.

As the new variant of Storm infects android devices, any work phones that use Android will have to be seized, imaged and turned off to ensure no meta-data is lost or overwritten by continued usage. If LiMe is used to retrieve the volatile memory off of the devices, the program can also provide a hash of the dumped memory, ensuring that it is not tampered with during the investigation. LiME also has a minimal process footprint, meaning that acquisition will not affect the data on the mobile device, keeping it forensically sound.

If Microsoft London makes use of cloud services, this could present a problem as there are jurisdiction complications as these services can be spread around the globe. Furthermore, these services cannot be preserved as these services must remain live and changeable for other clients to use. Physical access can also be an issue if the services are not near the investigator, and strict security requirements may make it difficult for an investigator to enter the premises.

Any log files from physical network devices should be stored on a remote server as these devices often have limited storage space, meaning that more comprehensive logs are available for the investigation.

Analysis

Once the data has been gathered and preserved, the analysis can begin. Here, fragments of data will be reconstructed. For network packets, this includes reconstructing the packets, and this can be done through Wireshark. Wireshark has a 'Packet Reassembly' feature which is used when the underlying protocol cannot handle large chunks of data. HTTPs or TLS protocols often space multiple TCP segments due to their size. Wireshark takes these segments and marks them all together as "[TCP segment of a reassembled PDU]". Additionally, if TCP segments are out of order, Wireshark can reassemble them in order.

Attempts will be made to recover any corrupt or deleted files using the meta-data on the devices that would have been secured during the preservation stage. During this phase, it is imperative that all work is carried out on the copies of the devices as discussed in the preservation phase. Autopsy is a digital forensics platform that allows the deployment of the Sleuth Kit, a collection of command line tools used to investigate device images. One of Autopsys' features is that it can recover deleted files from unallocated space. Meaning that any attempts to hide Storm can be recovered. Any

changes made to files on the original devices will be fully documented, including how it was changed and why. Screenshots and photographs of the devices will be taken for the documentation phase.

As data reconstruction begins, the investigator can start drawing conclusions on how the botnet has affected the network and what devices are infected. Using the timestamps from logs and captured packets, the investigator can begin drawing up a timeline of events to see how the botnet has initially infected the network and how it has spread.

Documentation

This phase happens throughout the investigation and continues after the investigation, making it the first post-investigation phase. Once all the data has been analysed, and a timeline has been established, all of the work will be documented and recorded. The point of documentation is to recreate how the network was infected and how that infection spread. The documentation will be in the form of a report detailing a timeline of events, screenshots and photographs of evidence, overall findings of the investigation and a discussion of countermeasures to be put in place for future breaches.

Logs from physical devices such as routers and switches and packet captures will assist in creating an entire timeline. The status of devices at acquisition will also be noted. Any important files will be documented with their whole file system paths. Network data will be recorded with their source and target addresses at the various network layers. Any devices that were acquired will include when and where they were seized. As well as recovering deleted files for the analysis stage, Autopsy can be used to create a timeline of events on physical devices, and it does so in a graphical format.

Presentation

Once the botnet has been identified and documented, the entire investigation will be summarised and explained at a lower level, meaning that any technical aspects will be wholly described to help understand the full extent of the investigation. For example, Autopsy creates a timeline of events on a device in a graphical format, making it easier to describe. Explaining it this way will allow all relevant persons at Microsoft London to be prepared to discuss the next steps and be entirely informed of the situation. Finally, recommendations will be made regarding the current state of the network and the relevant devices and how the company should proceed based on the findings of the investigation.

Discussion and Findings

Having a botnet within the network can have profound implications for Microsoft London as the legitimate user no longer has complete control of the infected machine, meaning that sensitive content stored on these devices becomes vulnerable. If this sensitive data is leaked, this could have significant consequences for Microsoft London, mainly if it includes information stored around users. Assuming the company is London based, they are legally obligated to abide by UK GDPR. One of the main principles of UK GDPR is 'Integrity and Confidentiality', which means that personal data should be appropriately secured. In the event of a data breach, the Information Commissioner's Office (ICO) must be made aware no later than 72 hours after becoming aware of the breach. Failing to notify the ICO comes with a substantial fine of up to £8.7 million or 2 per cent of the company's global turnover (Information Commissioner's Office, 2021). Additionally, if the botnet has control of multiple devices within the network, it can monitor the network and potentially collect extra data being sent to and from machines.

Suppose Microsoft London has a Botnet in its network. In that case, this can severely affect device performance because if the devices are used to perform malicious acts, this takes up resources on the device. For example, Botnets are commonly used to perform Distributed Denial of Service (DDoS) attacks. A DDoS attack uses the device's resources to send fraudulent requests. On a large scale, this overwhelms the victim's device and can cause it to crash from dealing with all the simultaneous requests. As this uses up resources, it makes fewer resources available for the legitimate user of the device, making it harder for employees to do their day-to-day tasks, therefore reducing productivity.

Further on from this, ensuring a network is secure from botnet attacks is more important now than ever due to 'Botnet Mining'. Botnet Mining is where infected computer hardware is used to mine cryptocurrency for a hacker (Seth, 2022). Although this doesn't directly take money from the victim, it does so in other ways, such as additional electricity costs from having the device running at full load. Additionally, the life span of the hardware can be reduced if it runs at high temperatures all day, meaning the device's parts (or the device itself) will have to be replaced sooner than expected.

There are several ways Microsoft London can reduce the chance of having a botnet infiltrating its network. The first and most common solution is to certify all software is up to date, as outdated software can leave the system vulnerable to attacks. Recently it was found that the 'Mirai' botnet (a botnet known for some of the most disruptive DDoS attacks) is being spread through a vulnerability called 'Spring4Shell'. This vulnerability allows attackers to perform remote code execution (running commands remotely) within a Java framework called Spring (Leyden, 2022). This vulnerability can be patched by upgrading the Spring framework. (Marr, 2022)

Another important method for protecting systems from botnets is to train staff to be more cyber-aware. Storm spread using a piece of malware called the 'Storm Worm'. Storm Worm was a type of malware called a 'Trojan Horse' which tricks users by pretending to be a legitimate attachment. The Storm Worm was found as an attachment in spam emails with enticing titles such as 'Russian missile shot down USA satellite' which encouraged users to download the malware onto their machines. Educating staff to be warier of spam emails and opening attachments from unknown sources can significantly reduce the chance of a network breach.

Monitoring network traffic is a great way to protect against botnets and other network breaches. Using a Network Intrusion Detection Service (NIDS) deployed strategically across the network, Microsoft London can gauge what normal network traffic looks like and create alerts based on abnormal network traffic. Having a log of real-time events is essential in case a malicious user tries

to cover their tracks and helps the company identify the entry point used. Additionally, a Host Intrusion Detection System (HIDS) can be paired with a NIDS to defend individual devices on the network. As stated earlier, the Storm Worm originally spread from a piece of malware attached to an email, a HIPS would detect that the program is trying to do something malicious and stop it before it effects the device. These two systems can be a very effective defence against malicious actors. (SEQRITE, 2018). Should Microsoft London already have a NIDS in place, its rules should be regularly updated, and the alerts generated should be analysed to ensure that the NIDS is being used to its full potential. Otherwise, there is no point in having a NIDS.

Conclusion

In this investigation, the aim was to assess the original Storm botnet and discuss how a forensic investigation would be taken to examine the new version of Storm. The investigation found what data sources which would have to be assessed to find evidence of Storm and how that evidence would be preserved to ensure its integrity. From there, the evidence is analysed, documented and presented in a non-technical format.

Along with the digital forensics investigation layout, this report has provided several countermeasures Microsoft London can implement now to protect its network from similar future attacks. Including educating staff on how to identify malicious attachments and ensuring their services are up to date to protect them from vulnerable software.

The findings of this research should assist Microsoft London in its decision to investigate the new version of Storm thoroughly.

References

Holz, T. et al., 2008. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. *Leet*, 8 April, pp. 1-9.

Ibrahim, M. & Jantan, A., 2011. A Secure Storage Model to Preserve Evidence in Network Forensics. *ICSECS,* 180(1), pp. 391-402.

Information Commissioner's Office, 2021. *Personal data breaches.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches
[Accessed 2 November 2022].

Leyden, J., 2022. *Attackers are abusing Spring4Shell vulnerability to spread Mirai botnet malware.* [Online]
Available at: https://portswigger.net/daily-swig/attackers-are-abusing-spring4shell-vulnerability-to-spread-mirai-botnet-malware
[Accessed 28 October 2022].

Marr, B., 2022. *Spring4Shell [CVE-2022-22965]: What it is and how to detect it.* [Online]
Available at: https://www.intruder.io/blog/spring4shell-cve-2022-22965
[Accessed 28 October 2022].

Naraine, R., 2007. *Storm Worm botnet could be world's most powerful supercomputer.* [Online]
Available at: https://www.zdnet.com/article/storm-worm-botnet-could-be-worlds-most-powerful-supercomputer/
[Accessed 11 November 2022].

Scanlon, M., 2013. Study of Peer-to-Peer Network Based Cybercrime Investigation: Application on Botnet Technologies. *University College Dublin*, 10 October, pp. 1-144.

Security Encylopedia, 2021. *What is the Storm Worm.* [Online]
Available at: https://www.hypr.com/security-encyclopedia/storm-worm
[Accessed 3 November 2022].

SEQRITE, 2018. *Benefits of having Intrusion Prevention/Detection System in your enterprise.* [Online]
Available at: https://www.seqrite.com/blog/benefits-of-having-intrusion-preventiondetection-system-in-your-enterprise/
[Accessed 31 October 2022].

Seth, S., 2022. *Botnet Mining.* [Online]
Available at: https://www.investopedia.com/tech/what-botnet-mining/#:~:text=Sachs%20and%20BlackRock.-,What%20Is%20Botnet%20Mining%3F,who%20is%20the%20remote%20attacker.
[Accessed 31 October 2022].