Microsoft London Forensic Investigation

Jack Sime

CMP416: Advanced Digital Forensics

BSc Ethical Hacking Year 4

2022/23

Note that Information contained in this document is for educational purposes.

.

Contents

1 Introduction 1
1.1 Background 1
1.2 Aim 2
2 Acquisition and Investigation strategy 3
2.1 Acquisition 3
2.2 Investigation Strategy Plan 4
2.2.1 Identification 4
2.2.2 Preservation 4
2.2.3 Analysis 5
2.2.4 Documentation 5
2.2.5 Presentation 6
3 Discussion 7
3.1 Tools 7
3.2 Prevention 7
3.3 Implications 8
4 Conclusion 10
References 11

.

1 INTRODUCTION

1.1 BACKGROUND

Microsoft London is currently being infected by a modern version of the Storm Worm that is targeting android phones and the newest version of windows. The original storm botnet was malware that was spread through the Storm worm using email spam and created a large network of remotely controlled computers (*What is the Storm Worm? | Security Encyclopedia*, no date). These computers could then be used as spam servers, part of a DDoS attack, or other functions. Whilst at its most prevalent during the late summer of 2007, Storm was spreading through email spam where users would be socially engineered into downloading the malware (Garretson, 2007).

Researchers believed that the Storm botnet was rentable in portions allowing people to take control of a set number of machines to carry functions such as sending spam emails with no traceable IP (Tung, 2007). The Storm botnet was dangerous due to its ability to spread easily through systems running a certain version of windows, its versatility with its multiple functions and the thought of corporate assets becoming part of the crime-committing botnet. Storm was also found to be a polymorphic virus, where its code would change or "mutate" (Schneier, 2007) which would increase its effectiveness in avoiding signature-based anti-virus detection making it harder to catch and would actively defend against anyone trying to reverse engineer it.

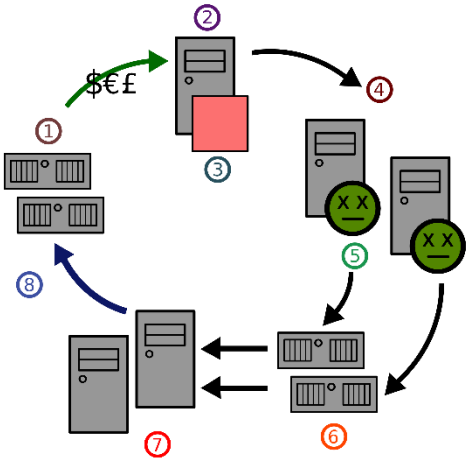

Figure 1: Storm Botnet Lifecyle

This report will cover the modernized version of Storm and how a forensics investigation would be performed in response to the updated version of Strom. The report will go into detail on potential data sources along with how the strategic flow of the investigation would be handled. The report will also discuss potential techniques that could be used to prevent the impact of the modern Storm botnet. The report will then be concluded with the overall findings of the report. The investigation would follow a

methodology from NIST on integrating forensics into incident response (Kent *et al.*, 2006) of Collection (Identification, Preservation), Examination, Analysis and Reporting (Documentation, Presentation).

1.2 AIM

This report aims to set out how an independent digital forensics investigator would carry out an investigation into an infection of a modernized Storm botnet. This overall aim comprises of a number of sub aims:

- Set out an investigation strategy to be followed
- Identify key data sources
- Discuss preventative measures and their implications

2 ACQUISITION AND INVESTIGATION STRATEGY

2.1 ACQUISITION

Before conducting any investigation into the ongoing Storm botnet, key data sources would be used to provide valuable information on how this modernized Storm malware is both functioning and spreading within the network. Data sources from the original Storm malware would be gathered along with further sources. These data sources will set the starting point for the investigation and obtaining these multiple data sources will provide multiple points of information on the network and devices within it.

For each data source, permission to access and capture the data would be requested ahead of carrying out the process of acquiring data.

Images of Infected PCs (Desktop & Servers) and Phones: Images of Infected devices would be taken to allow for the devices to be forensically analysed for information relating to how that device was infected as well as how it may have been used to infect further devices (Imam, 2019). Images of infected devices would also allow for a copy of the malware to be obtained that can be redeployed within a safe environment for further analysis.

Logs from Network devices (Switches and Routers): Logs from the network devices, such as any routers or switches, used within the Microsoft London network would be used to help identify any movement within the network that may have originated from an unknown device. This would help to identify any suspicious traffic that could be connected to the attack and would help in identifying the source of the infection.

Logs and Alerts from NIDS: Depending on the configuration and rules set up within the NIDS these logs and alerts would be used to help identify any anomalies within the network that may be related to the initial infection and the subsequent spread within the network. This would help to isolate affected machines and narrow down an initial point of infection.

Logs from PCs: Logs from both infected and uninfected systems would be used to help identify any key changes the malware may have made to its host device after it has been infected. This would allow for characteristics of the malware to be identified and could be used to further understand how the malware operates within the network and hosts.

Employee Email Logs: Logs from company email addresses would be used to help identify if the initial infection or any spread is being carried out via email once permission had been requested and accepted. They would also be used to identify any relevant spam campaigns or relevant phishing attempts that may have resulted in the initial infection or breach of a user account or the network.

Live Network data: Live network data would allow for live connections and traffic to be captured that could then be analysed to analyse any suspicious connections and/or traffic incoming or outgoing from any system on the network. A list of the known IP addresses from within the network would allow for unknown IP addresses to be quickly identified.

2.2 INVESTIGATION STRATEGY PLAN

2.2.1 IDENTIFICATION

Using the data sources that were previously listed as potential sources of valuable information, devices that correspond to the listed data sources would be identified within Microsoft London and would be noted down for further identification of the data present on the device. After identifying the suitable devices located within the company, the data present on these devices would then be identified along with key details relating to the information such as how and where it is stored on the device or network along with its condition. These steps ensure that the data can be quickly located and will allow for the isolation and preservation of the data that is relevant to the investigation. Identifying how the information will be stored for analysis is also considered here to ensure that the data remains forensically secure and identical to the source.

2.2.2 PRESERVATION

To preserve the integrity of the PC's images that are noted in the data sources several different tools would be used to gather the images and required data. Where possible Live captures will be performed on machines rather than a dead capture (Kolhe and Ahirao, 2017). The tool FTK imager would be used to capture both volatile memory and non-volatile memory within the target PCs. The software would be operated from a portable drive and would allow for more information to be gathered as the volatile memory contains key information such as network connections and processes running at that time (Fox, 2021). Where machines are not currently online, a dead capture would be performed. The drives from the computer would be removed and inserted into a drive bay connected to a hardware write blocker to ensure the drive is not altered. FTK imager would then be used again to copy the non-volatile memory from the drive. Checksums of the images would be taken at the start and would be used to ensure image integrity throughout the investigation (Scanlon, 2013).

Log files mentioned within the data sources would also be isolated and preserved forensically to ensure that they are not altered or changed in any way. Checksums of these logs will also be taken to improve integrity when comparing them before analysis with during and after analysis. The logs will then be stored securely to be later analysed for valuable information.

Live network traffic captured within the network would be captured using Wireshark and/or tcpdump and would be stored as pcap files that can later be analysed to identify suspicious connections.

Phone data would be isolated by restriction the target device's access to outside connections to prevent the data on the device from being altered. A bit-by-bit copy would be produced for any mobile devices that may be relevant to the investigation (Envista, no date). The phone would be connected using a

write blocker to prevent any of the data from being altered and each device would be checked for external memory cards also to be imaged (Lessard, Kessler and Associates, 2010).

2.2.3 ANALYSIS

After preserving the extracted data, the copies would then be analysed using a range of tools allowing for relevant data to be investigated and for irrelevant data to be filtered out. To investigate the volatile memory that would be captured during live captures, the tool volatility would be used as it would allow for the information stored within the volatile memory of machines to be investigated. Any active network connections revealed within the volatile memory can then be cross-referenced with NIDS alerts and Wireshark data to narrow down any suspicious traffic that may reveal information on the spread and how it potentially started.

The forensic tool Autopsy would be used to investigate the images of the non-volatile memory (Drives) and the mobile phone images that were gathered during preservation. Autopsy would allow for the contents of the drive images and phones to be searched for suspicious files on machines or any changes that had been made to files present on the machines or phones at the time of being imaged. Autopsy would also be used to look at the email data that would have been collected.

Live traffic captures that had been stored within pcap files would be analysed using both Wireshark and tcpdump to successfully read the captured files for analysis. These applications would allow for connections to be analysed and would facilitate the further analysis of connections that are identified to be suspicious and the contents of the requests. Information such as ports used by the botnet and extensively used IP addresses could be identified to be used in preventative measures. Ngrep and HxD would be used where necessary to search gathered traffic for specific strings and allow for files located within traffic to be carved.

Logs and alerts from any NIDS's deployed within the network would be investigated using both grep and tcpdump to locate alerts that have been caught by the NIDS along with matching the packets related to the alert so that they can also be analysed.

Any samples of malware found would be analysed in a controlled environment such as a VM to understand how it functions and how it may spread. The network attempts from the malware would be monitored using Wireshark. The tool Ghidra would be used to investigate the malware and disassemble the sample to further work out how it functions. PeStudio would also be used to investigate any malware samples as it would allow any strings and other artefacts to be extracted from the sample and compares the hashes of the sample to known samples provided with VirusTotal. This would allow the identification of any new additions to the Storm malware when compared to the older version of Storm.

2.2.4 DOCUMENTATION

Using the results obtained from careful analysis of the gathered information, a network map detailing the process of how Storm spread through the network would be created. This map would detail the origin point of the network's infection and would follow the trail of infection within the network allowing for a clear path of infection to be established. This would also allow for areas to be identified that require additional security or that require reconfiguration.

A timeline of the events relating to the infection would be produced from the gathered research and would provide a clear understanding of the events that occurred during the infection and spread.

2.2.5 PRESENTATION

Upon competition of the investigation, a fully compiled report of the details relating to the investigation, such as the steps taken within the investigation including any tools that have been used and the overall outcome of the analysis that has been performed, along with the components detailed in the documentation section will be supplied to the Microsoft London. This report would also contain recommendations on vulnerable areas of the network that should be addressed.

A brief alternative report or presentation will be produced and be available for presentation to executives within Microsoft London to summarize the events of the investigation along with the key findings from the analysis and the critical changes that should be implemented to help prevent an attack of this nature from happening again.

3 DISCUSSION

3.1 TOOLS

FTK imager was chosen for usage within the forensic process as it is an effective tool for imaging drives and capturing volatile memory (RAM). The portable version of FTK imager would be used as it can be used from a portable drive instead of installing it on the target machine. Being able to capture both memory types using one tool saves time and can reduce the number of steps required during an investigation (Chandel, 2020). After an image is created the hash is calculated and can be used to ensure the integrity of the file.

Autopsy was selected for usage when investigating the drive and mobile device images where it is useful for investigating any files that may have been edited or added to a device's memory. Autopsy allows for files to be easily searched within the image and can create a timeline of system events that is easy to understand and read.

Both Wireshark and tcpdump were chosen to be used for live traffic capturing and analysis. Wireshark allows for a wide range of information to be gathered on active traffic and allows for filters to be used within a set of data to on information that may be suspicious, this allows for relevant data to be focused on and allows for easier analysis of known suspicious IP addresses or specific protocols. Wireshark would also be used to extract potential files located within suspicious requests along with providing key details about the selected packets. Both tcpdump and grep allow for searching through the alerts and logs produced by a NIDS and can be used to isolate details relating to the target of the investigation and can be used to gather details on specific alerts and logs containing specific details.

Ngrep and HxD were selected for usage when analysing packets and their contents alongside Wireshark as Ngrep can be used to search pcap files for specific words that may have been identified and that may be related to the investigation whilst HxD would be used where files and data found within the captured traffic need to be carved to obtain the original file that may contain important information.

3.2 PREVENTION

Depending on the discovered method of initial entry and infection multiple avenues of prevention would apply to the situation. Due to the nature of the original Storm malware that updated itself and actively defended itself, 100% prevention would be difficult to achieve but these measures would help to limit both the spread and the impact of an infection.

Employee social engineering training would be a useful prevention measure if the initial point of infection were found to have come from a phishing or social engineering attack as seen with the original Storm malware (securitymetrics, no date). Ensuring employees understand the dangers of phishing emails and can successfully spot them can reduce the chance of infection through a spam email attack. This training would also prevent the spread through mobile devices (Flø and Jøsang, 2009) by giving

employees the training to also identify suspicious SMS messages that may be used instead of email. Also ensuring employees understand the risks of suspicious downloads and prompts online can help to prevent social engineering attacks.

Implementing new rules into the active IDS system, which have been created using the information gathering and analysis conducted on network traffic previously, would allow the active IDS to detect the presence and operation of the botnet more effectively (Saiyod *et al.*, 2018). These rules would be implemented and evaluated within a controlled environment to ensure that they effectively detect the botnet's presence and correctly issue an alert. As botnets can change and many operate in different ways the rules would need to be regularly updated and evaluated.

Tweaking any firewalls present within the network to block/drop outgoing connections directed towards identified IP addresses related to the botnet will prevent the botnet from receiving main commands from the lead machine. This would limit the botnet's functionality and will help ensure the botnet activity is neutralised until devices can be cleaned.

The implementation of a contact tracing framework would allow for the botnet to be quickly detected and prevented from developing (Huang, Zeng and Liu, 2010). The framework would evaluate peers and assess their condition by looking for suspicious symptoms of infection. Once the contact chains reach a set threshold, nodes confirmed to be infected through the contact chain can then be treated to prevent the formation of the botnet and in turn its impact.

Ensuring systems are updated to the latest version containing the latest security patches would ensure that any vulnerabilities that have been discovered by manufacturers or software developers are patched and are not available to exploit. This will reduce the chance of the network being infected by removing older and known vulnerabilities that will be patched through the updates received.

Deploying honeypots within the network would provide an effective way to detect the presence of malware spreading through the network (Wang and D'Cruze, 2021). The honeypots would present as regular devices within the network would detect when they have been triggered and would alert system admins to the presence of the infection (*What is a honeypot?*, 2022).

3.3 IMPLICATIONS

The preventative measures recommended above, and the impact of an infection would have different types of potential implications.

Social engineering awareness training would both have a financial implication and an environmental implication. The training itself would have to be paid for by Microsoft London and the overall office environment would be changed as people are reminded to be vigilant for attacks and are given the confidence to come forward should they think they have been impacted.

Microsoft London could suffer reputational damage if it was to be known that they had been breached by Storm and they may also face financial implications should of their devices be found to have taken part in any illegal activity from the botnet.

Any increase in security or alteration to the company's network would have both a financial and environmental impact as upgrading infostructure would require spending money to add or replace systems and would also potentially require further training to IT staff and changes to routines.

4 CONCLUSION

In conclusion, after researching the previous iteration of the Storm malware and the functionality of it multiple key data sources would be selected to be preserved and then analysed using specific appropriate tools that would provide valuable information on key areas of the new Storm malware such as any changes to its infection methods. The integrity of each data source would be ensured through hash calculation before analysis and with regular comparisons to ensure nothing had been altered.

From the analysis, multiple different preventative measures would be recommended to be implemented that would be designed to both prevent infection and help to reduce the impact should an infection occur. The report including the suggest preventative measures along with their implications would be presented to Microsoft London within a detailed report after the investigation would be concluded.

REFERENCES

Chandel, R. (2020) 'Comprehensive Guide on FTK Imager', *Hacking Articles*, 6 November. Available at: https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/ (Accessed: 6 November 2022).

Envista (no date) *Mobile Device Forensics and Cell Phone Experts | Envista Forensics*. Available at: https://www.envistaforensics.com/services/digital-forensics-services/mobile-phone-forensics/ (Accessed: 6 November 2022).

Flø, A.R. and Jøsang, A. (2009) 'Consequences of Botnets Spreading to Mobile Devices', p. 7.

Fox, N. (2021) *Memory Forensics for Incident Response*. Available at: https://www.varonis.com/blog/memory-forensics (Accessed: 30 October 2022).

Garretson, C. (2007) *Storm: the largest botnet in the world?*, *Network World*. Available at: https://www.networkworld.com/article/2286172/storm--the-largest-botnet-in-the-world-.html (Accessed: 26 October 2022).

Huang, Z., Zeng, X. and Liu, Y. (2010) 'Detecting and blocking P2P botnets through contact tracing chains', *International Journal of Internet Protocol Technology*, 5(1/2), p. 44. Available at: https://doi.org/10.1504/IJIPT.2010.032614.

Imam, F. (2019) *Common mobile forensics tools and techniques*, *Infosec Resources*. Available at: https://resources.infosecinstitute.com/topic/common-mobile-forensics-tools-techniques/ (Accessed: 6 November 2022).

Kent, K. *et al.* (2006) *Guide to integrating forensic techniques into incident response*. 0 edn. NIST SP 800-86. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-86. Available at: https://doi.org/10.6028/NIST.SP.800-86.

Lessard, J., Kessler, G.C. and Associates, G.K. (2010) 'Android Forensics: Simplifying Cell Phone Examinations', 4, p. 12.

Saiyod, S. *et al.* (2018) 'Improving Intrusion Detection on Snort Rules for Botnet Detection', *Software Networking*, 2018(1), pp. 191–212. Available at: https://doi.org/10.13052/jsn2445-9739.2016.011.

Scanlon, M. (2013) 'Study of Peer-to-Peer Network Based Cybercrime Investigation: Application on Botnet Technologies'.

Schneier, B. (2007) *The Storm Worm - Schneier on Security*. Available at: https://www.schneier.com/blog/archives/2007/10/the_storm_worm.html (Accessed: 26 October 2022).

securitymetrics (no date) *Social Engineering Training: What Your Employees Should Know*. Available at: https://www.securitymetrics.com/blog/social-engineering-training-what-your-employees-should-know (Accessed: 6 November 2022).

Tung, L. (2007) *Storm worm botnet threatens national security? | ZDNET*. Available at: https://www.zdnet.com/article/storm-worm-botnet-threatens-national-security/ (Accessed: 26 October 2022).

Wang, P. and D'Cruze, H. (2021) 'HONEYPOTS AND KNOWLEDGE FOR NETWORK DEFENSE', *Issues In Information Systems* [Preprint]. Available at: https://doi.org/10.48009/3_iis_2021_259-272.

What is a honeypot? (2022) *www.kaspersky.co.uk*. Available at: https://www.kaspersky.co.uk/resource-center/threats/what-is-a-honeypot (Accessed: 6 November 2022).

What is the Storm Worm? | Security Encyclopedia (no date). Available at: https://www.hypr.com/security-encyclopedia/storm-worm (Accessed: 26 October 2022).