Storm Botnet 2022 Investigation

Forensic Research and Suggested Countermeasures Report

Nick Nesterenko

CMP416: Advanced Digital Forensics: Coursework 1

BSc (Hons) 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
1.3 Overview of the Methodology 2
2 Acquisition and Investigation Strategy 3
2.1 Obtain Information 3
2.2 Strategize 4
2.3 Collect 4
2.4 Analyse 5
2.5 Report 6
3 Discussion and Findings 7
3.1 Storm Botnet 2007 Brief Analysis 7
3.2 Network Forensic Tools 8
3.3 Countermeasures 9
4 Conclusion 10
References 11

1 INTRODUCTION

1.1 BACKGROUND

Bot-Networks (Botnets) are groups of infected interconnected hosts controlled by a malicious threat actor. Usually, botnets are controlled by a Command and Control (C&C) server, the C&Cs can distribute the instructions to be performed ubiquitously within the botnet network (Thanh Vu et al., 2021). Botnets can be used for a variety of reasons such as distributed denial-of-service (DDoS) attacks, spam distribution, brute-forcing and many more. Every day, botnet malware becomes more advanced, in summer 2022, the Mantis botnet, as noted by Cloudflare, managed to reach 26 million requests per second by just 5000 infected hosts, which was not possible just under a decade ago (Yoachimik, 2022).

Generally, there are two main ways of how botnets are controlled. In **Decentralised** or **Peer-to-Peer (P2P) Architectural Structure** (Figure 1), the bot instructions are distributed by the bots themselves after one of the bots receives the commands from C&C server. On the other hand, in **Centralised Architectural Structure** of botnets (Figure 2), all bots are controlled solely by the C&C server. The architecture differences between the two types of botnet structures have their advantages and disadvantages. The centralised botnets can be more efficient, however P2P botnets are much more resilient to countermeasures which makes it a more significant threat to large companies as the botnets can cause significant disturbance without being noticed/being harder to prevent (Thanh Vu et al., 2021).

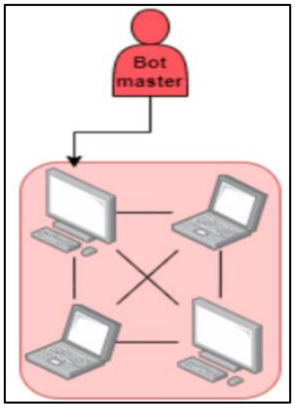

Figure 2: Example of a decentralised (P2P) C&C botnet structure (Thanh Vu et al., 2021)

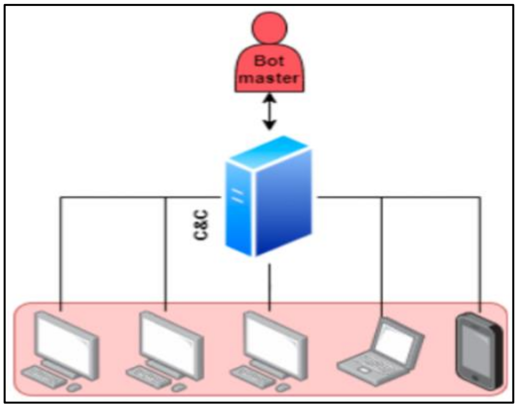

Figure 2: Example of a centralised C&C botnet structure (Thanh Vu et al., 2021)

One of the famous examples of largest P2P botnets is the 2007 Storm botnet. In January 2007, the Storm botnet/worm was first detected on the internet. At the time it was considered an evolution of botnet malware, dragging attention of various security experts. It mainly spread through phishing emails which described various weather accidents, hence the name “Storm”. The threat actors developed a complex piece of software which involved multiple techniques such as detection evasion, polymorphic code, peer-to-peer connections, social engineering and more. The total number of infected machines is uncertain, but it would be measured in millions of infected machines. As of September 2007, Storm botnet was referred as “the largest botnet in the world” at the time, and the estimated number of infected systems was over 1 million (Garretson, 2007). In late 2008, Storm botnet’s activity declined for few reasons like identification of several C&C servers as well as the *Stormfucker* software which utilised the exploit which allowed to control segments of the botnet (Eliot, 2009).

It is now 2022, 15 years later, the Storm botnet is back, it is now modernised and targeting the newest versions of Windows, and some evidence suggest that Android based systems may be targeted. Strom 2022 spreads through computers through the local network. Microsoft's new London headquarters shared the concerns about the matter and requested additional information about the botnet through an investigation and possible countermeasures which were detailed in this report.

1.2 AIM

Considering the said above, by investigating Storm, it was planned to hand over the following information to Microsoft in a form of report which will be used as a consultation during the stage of decision making:

- Brief analysis of Storm 2007.
- Ways to adapt to the new variant of Storm.
- Coverage of all stages of digital intruder investigation, including the justification of relevance of findings and suggestions.
- Possible countermeasures for Microsoft London's network.
- Likelihood of finding and shutting down the new version of Storm.
- Suggested preventive measures for future similar attacks.

1.3 OVERVIEW OF THE METHODOLOGY

For the purposes of this investigation, it was decided to use *OSCAR* methodology. This methodology was chosen over the more classic solutions (i.e., identification, preservation, analysis, documentation, and presentation) as it is a known, more modernised, and industry standard methodology. It is also important to note that OSCAR methodology focuses on *Network Forensics* which is relevant for Microsoft London's investigation and botnet topic. The use of OSCAR will ensure accurate and meaningful results as well as could potentially be more attractive to Microsoft London's stakeholders (Jaswal, 2019):

1. **O** – Obtain information. Learn about the incident and targeted environments.
2. **S** – Strategize. Plan the investigation based on information gathered.
3. **C** – Collect. Acquire the evidence as per plan.
4. **A** – Analyse. Analyse acquired evidence using different techniques eliminating false positives.
5. **R** – Report. Produce the investigation, must be in layman's terms.

This methodology was explored and described in detail in Section 2.

2 Acquisition and Investigation Strategy

2.1 Obtain Information

The first stage of the investigation would be the information gathering about the incident. As of the time of writing this report, the incident in Microsoft London's office did not yet occur, therefore, it was decided to describe the possible ways of preventing and mitigating the risks related to the new version of Storm in 2022. One of the initial stages of information gathering would be obtaining permission to conduct the on-site investigation to avoid any legal disputes. The investigation must not infringe any regulations or laws of the United Kingdom and avoid any possible misconduct (ENISA, 2022).

After the permission is provided, it is generally advised to *identify* the incident, time, date, and how it was discovered. Other information must be gathered as well such as the actions taken since the discovery, summary of internal discussions within the Microsoft London's office, the time frame for the investigation and recovery, and other investigation goals. During this phase it is also very important to know the data that can be lost during the attack as large companies such as Microsoft store a lot of sensitive personal information about their clients which can lead to legal issues if compromised. The main goal of this phase is to familiarise the investigator with the type of incident and provide a clear picture of the event. The suggested information to be gathered that was mentioned above refers to the general practices and some other customisation would be required as new information comes in if Microsoft London is compromised by Storm 2022 (Davidoff and Ham, 2012).

As the incident did not occur yet, there was a limited amount of information provided about the Storm 2022. However, the information about the 2007 version was available from public sources (See Section 3.1). It is still uncertain on who could be the threat actor who developed and controlled the 2007 Storm botnet, therefore the assumption that the person/organisation responsible for the modernised version of Storm is the exact same threat actor may be inaccurate. For example, it was discovered that the main mode of spread of the 2007 Storm malware was mainly through phishing emails which consisted of forecasted incidents such as hurricanes and storms themselves, therefore it would be logical to monitor the incoming emails of such content for all employees of Microsoft London. At the same time, spread through emails tends to be less popular nowadays but does exist in 2022 according to summary of modern trends in botnet design. Information about the network topology as well as available resources (such as equipment, number of employees, funding, and time) would also be meaningful as during the planning stage it would be helpful to understand and pre-plan the quarantining of infected systems and recovery process (Davidoff and Ham, 2022). Any other related available information about the environment of Microsoft London's office needs to be gathered at this stage based on the availability as per the time of this report, the internal information about the office's network structure and connected devices (servers, computers and IoT devices) was not known.

2.2 Strategize

When developing the strategy for forensic network investigation it is important to form a detailed plan of how the investigation would be carried out, this would be especially important considering the scope as Microsoft offices are usually large in size and utilise a significant number of interconnected devices including the experimental hardware and IoTs which may have limited security features.

At this stage, the time frames for the investigation and investigation goals must be set. The duration of the investigation would depend on the number of network hosts on-site and number of users/employees in Microsoft London's office. Therefore, it would also be beneficial to have the list of available resources, which should be completed during the *Obtain Information/identification* stage (See Section 2.1). After examining available resources, it would be possible to schedule the goals of the investigation and identify the possible data sources which would help the investigation. During strategizing, the sources of potential data sources must be noted down using the following format which will allow for further resource monitoring (Table 1):

Table 1: Example of evidence sources prioritisation (Davidoff and Ham, 2012)

Source of Evidence	Predicted Value	Costs	Volatility	Priority
Firewall logs	High	Medium	Low	2
Web proxy cache	High	Low	Medium	1
ARP tables	Low	Low	High	3

Prioritisation of evidence sources would be highly beneficial for time and cost management which will also lead to better reporting to Microsoft's stakeholders during the investigation process as it will show the confidence of the investigation and limit the panic levels. With that said, it is also important to plan the method and times of regular communication/updated on the investigation as well as the target audience (i.e., client and/or investors) (Davidoff and Ham, 2012). It would also be advantageous to plan the training of the employees to watch for any device and network anomalies as well as phishing emails related to extreme weather conditions. Getting the idea of possibilities of data preservation and possible attack vectors such as opened ports would also be beneficial for further data *preservation* and quarantining of infected systems. Keep in mind that due to the scope of the investigation at Microsoft, the strategy development would have critical importance for the distribution of work and coordination of the investigation team.

2.3 Collect

One of the most sensitive and resource dependent phases of the investigation would be the *evidence collection and preservation.* At this stage, the clear plan of the investigation must be complete. To minimise costs, the collection of evidence should, but not must, begin after the cyber incident occurred, in this case, there must be some spiculations that the 2022 Storm malware has entered the network of Microsoft London. At the time of this document's creation, the information about the evidence sources availability was not known, however, the following table demonstrated the probable sources of evidence which could be used during the investigation (Table 2):

Table 2: Possible evidence from the end or intermediate devices (Qureshi et al., 2021)

Affiliation	Source
End side (attacker and/or victim side)	Operation system audit trail, system event log, application event log, phishing email filtering log, alert log, recovered data, and swap files
Intermediate	Traffic data packets, firewall log, IDS log, router log, and access control log

There are few vital components which should be considered during the investigation process. **Documentation**, all actions completed throughout the investigation must be documented and described including the time and date of the event that is being noted. The notes could later be used during the court case if the threat actors who developed Storm 2022 would be found as well as the insurance companies, therefore it is critical for minimising costs and risks of during the recovery process. The documentation should include information such as, time, source of evidence, method of acquisition, as well as the name of the investigator. (Qureshi et al., 2021).

Capturing, evolves the data isolation and *preservation* of devices to ensure the integrity of collected evidence as well as to limit the spread of the malware through the Microsoft network. This step also evolves the actual collection of the evidence in accordance with the pre-made strategy. See Section 3.2 for the overview of suggested forensic tools for evidence gathering.

Store/Transport, ensure that the evidence is stored securely, backed up and the chain of custody is maintained. The log of each seized evidence is well documented for further use (Jaswal, 2019). The backups should be stored in accordance with the Microsoft's manifest.

2.4 ANALYSE

Typically, the analysis process during forensic network investigations is not linear as it is case specific based on the acquired evidence, however there are several steps which should be considered. It is important to mention that the analysis should not be done on the active/live hosts but on the obtained copies to ensure there is no data lost such as random access memory data. Please, refer to Section 3.2 for the list of forensic analysis tools.

Correlation, the first step of the analysis where the data from multiple sources of evidence would be considered. It is important to note the sources of the evidence for the purposes of locating the correlation between the seized data (Davidoff and Ham, 2012).

Events of interest, some events during the investigation will be noticeably more relevant and significant than others. To minimise costs and help the progress of the investigation it could be considered to alter the plan of the investigation based on the located *events of interest.*

Corroboration, there would be a major chance of the quality of data that most of the networking logs consist of which may lead to "false positives". It would be advisable to corroborate the findings of network log analysis with analysis of other evidence sources to ensure accurate results (Davidoff and Ham, 2012).

Recovery of additional evidence, during the analysis, it is inevitable that there would be some instances of lack of evidence to progress through the analysis as it may lack sufficiency. Microsoft London must acknowledge that there could be a need to recover additional evidence during after the collection of evidence is considered complete.

Interpretation, the competent assessment of the collected evidence. Considering that the investigation would be conducted with the help of Microsoft’s security specialists, it would be less challenging understand the used techniques by the 2022 Storm botnet, however this step must be completed with special attention as it may help Microsoft to develop security patches to Windows systems.

2.5 Report

The final and one of the most important stages of the investigation. The relevance of previous steps would have no value unless documented and presented correctly. Poor documentation could lead to refusal of insurance issued funds for restoration of the operation of the office after being compromised by 2022 Storm variant. The bad presentation could also harm Microsoft’s public image which will drag the concerns of competence of investors and clients etc.

The report produced after the investigation is completed must be written in non-technical language to be understood by legal teams, managers, investors, governmental agencies, clients, media, and other stakeholders. It is important to note that due to the respectability of Microsoft, the investigation report which would be published for public use would also be used by other companies and individuals to combat Storm 2022, therefore, not only the results of the investigation should be published but also suggestions must be shared too.

3 Discussion and Findings

3.1 Storm Botnet 2007 Brief Analysis

Storm botnet was spotted in 2007, at the begging, it spread using phishing emails containing videos of destruction caused by a recent weather incident in Europe and other weather-related information. It was “one of the most advanced” malware at the time as it utilised several new techniques which was not used by the malware priorly. Strom was used mainly to produce spam emails, and which promoted fake medical drugs and other illegal goods. Later in the malware lifecycle, the Storm bots were rented out to perform variety of computational tasks such as DDoS attacks (Smith, 2008). In mid 2007, Storm was responsible for the 20% of all spam on the internet (Balaban, 2022). During the year of 2007 Storm botnet managed to send over 1 billion email messages which was also used for spreading (Figure 3):

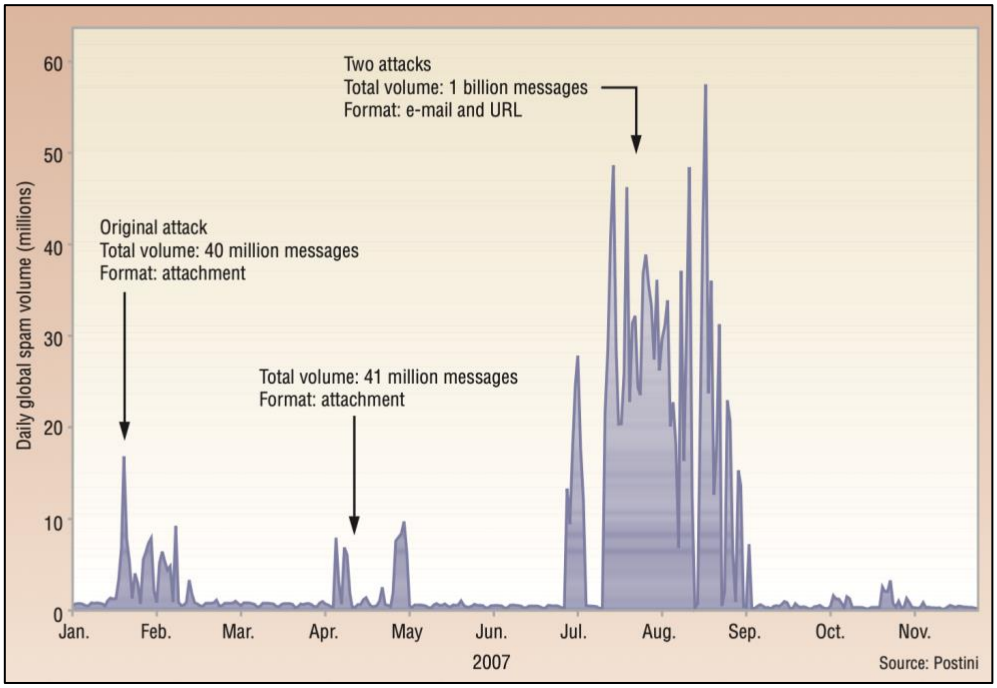

Figure 3: Numbers of messages sent by Strom in 2007 (Smith, 2008)

It was the defence mechanisms that made Strom resilient lead to its notorious success. One of the methods of self-preservations was the fact that it was a decentralised botnet which made it difficult to locate the bot-master computer. Storm also inactive for most of the time which allowed it to stay undetected while a limited number of bots self-propagated, lowering the risks of complete deletion from the infected network. The malware also used a complex 40-bit encrypting which was very challenging to decrypt at the type, this lowered the chances of being detected through the automatic network traffic analysis. Storm also used a technique called code replacement; the bots would replace the core code up to 10 times per hour which dragged challenges of identification by anti-virus software. The combination of those facts made Storm very difficult to combat, left alone the P2P Overnet protocol which was used by the bots to communicate instructions (Smith, 2008).

3.2 Network Forensic Tools

The use of trusted and tested network forensic tools assist the investigation to gather the evidence and progress faster through the detection and investigation. There are many tools with different functionality which have their advantages and disadvantages. The choice of tools for the investigation is generally case based, however there are several tools which could be called essential.

Wireshark. An open-source GUI software used for capturing, filtering and analysis of the network traffic. The main advantage of it is the intuitive user interface which accelerates the investigation in comparison with the command line alternatives such as *tcpdump* which relies more on manual analysis. Wireshark is able to examine the network packets in real time as well as provides the decoding protocol capabilities, and packets detail markup language. The general use of Wireshark includes the evaluation of the structure of the network traffic and checking for potential security flaws. Wireshark is one of the main tools when it comes to network forensics, as it is open source there is ability to install plugins to expend the functionality even more. This tool can be used throughout the investigation process as well as manual detection.

Snort. Another opensource tool which is used as a Network Intrusion Detection System (IDS) and prevention system (IPS). Currently, Snort is developed by Cisco, one of the largest networking solutions providers, which assures the credibility of the tool. This tool can be used to detect device fingerprinting, attack attempts, and many more. Snort can be used in three different modes:

1. Sniffer mode – like Wireshark, displays the network traffic.
2. Packet logger mode – logs network traffic onto the storage device.
3. Network Intrusion Detection System Mode – monitors the traffic and analyses it against the preconfigured rules.

The most powerful feature of Snort would be the ability to monitor traffic based on configured rules. Correct configuration could increase the security of Microsoft London’s network significantly without the loss of the functionality of the network for business purposes.

There are many other tools which can be used for network forensics and to combat botnets, the following table showcases the list of tools which Microsoft could consider for using during the investigation (Table):

Table 3: Commonly used tools during network forensic investigations (Qureshi et al., 2021)

Tool	Website
Tcpdump	www.tcpdump.org
Ngrep	ngrep.sourceforge.net
Driftnet	www.backtrack-linux.org/backtrack-S-releue
NetworkMiner	www.netresec.com/?page=NetworkMiner
Aircrack-ng	www.backtrack-linux.org/backtrack-S-releue
Kismet	www.kismetwireless.net
NetStumpler	www.netstumbler.com
Xplico	www.packetstormsecuity.org/files/tags/forensics
DeepNines	www.deepnines.com
Sleuth Kit	www.sleuthkit.org

Argus	www.qosient.com/argus
Fenris	camtuf.coredump.cx/fenris/whatis.shtml
Flow-Tools	www.splintered.net/sw/flowtools
EtherApe	etherape.sourceforge.net
Honeyd	www.citi.umich.edu/u/provos/honeyd
Snort	www.snort.org
Wireshark	www.Wireshark.org

3.3 COUNTERMEASURES

Several countermeasures can be used to combat Storm 2022. An effective method to prevent the spread of the Storm malware would be successful detection mechanisms. Not only early detection will be able to limit the infection levels but also to understand the techniques used by the malware.

Firstly, as 2007 Storm used to be spreading using phishing emails, the SMTP analysis would be a feasible countermeasure. SMTP analysis technique would help Microsoft to catch the text and image-based botnet spam emails, however, many emails could be falsely flagged. This method also has a high detection rate which could help prevent the phishing emails to spread amongst the employees of Microsoft London.

Packet filtering would also be effective as even after the infection, the filtering mechanisms can be used to prevent the botnet to communicate with the botnet master and receive the instructions which could lead to lower number of associated risks.

Reverse engineering could be an effective way to tackle Strom 2022. Due to availability of the resources to Microsoft's security team and the level of expertise. A sample of the malware could be reverse engineered in a protected environment which would lead to better understanding of operation of the botnet.

The DNS traffic monitoring could assist in detection of known and unknown botnets by monitoring DNS traffic anomalies. This method requires a lot of computation powers which Microsoft is capable of using due to the access to the Azure cloud computing. However, it the feasibility would be debatable until the associated risks with Storm 2022 are evaluated.

Regarding the spiculations that the malware may target Android devices. The dynamic real-time analysis can be used to identify botnet malware on the device. The dynamic analysis will help to identify anomalies in the operation of the .apk file which would suggest whether the device of an employee is infected or not which would assist the prevention of further spreads.

4 CONCLUSION

Overall, this report demonstrates the suggested network investigation structure in relation with the Microsoft London's concerns regarding the new variant of Storm botnet malware. All essentials of the network investigation (identification, preservation, analysis, documentation, and presentation) combined with OSCAR methodology, Microsoft should have a better understanding of the actions that would be required in case of infection by Storm 2022. The steps provided should also limit the risks associated with the potential infection as well as help evaluate the implications.

The brief analysis of 2007 Storm version should also provide understanding regarding the 2022 Storm version, assuming the threat actors use some of the techniques which were used in 2007. The provided countermeasures should also help Microsoft London prevent the infection at the first place, or at least improve the detection time frames.

By conducting the network investigation in accordance with this report Microsoft should gather the necessary intel more efficiently for further development of security patches for Windows products, and help the public understand the threat implications and countermeasures better.

REFERENCES

Mattwojo (2022) *Windows dev kit 2023 (project volterra)*, *(Project Volterra) | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows/arm/dev-kit/ (Accessed: November 7, 2022).

Yoachimik, O. (2022) *Mantis - the most powerful botnet to date*, *The Cloudflare Blog*. The Cloudflare Blog. Available at: https://blog.cloudflare.com/mantis-botnet/ (Accessed: November 7, 2022).

Eliot (2009) *Tagged - stormfucker*, *Hackaday*. Available at: https://hackaday.com/tag/stormfucker/ (Accessed: November 7, 2022).

Jaswal, N. (2019) Hands-on network forensics: investigate network attacks and find evidence using common network forensic tools. 1st edition.

Forensic Analysis Network: Incident Response Toolset, Document for students (2022) *ENISA*. Available at: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (Accessed: November 8, 2022).

Davidoff, S. and Ham, J. (2012) Network forensics: tracking hackers through cyberspace. Upper Saddle River, NJ: Prentice Hall.

Balaban, D. (2022) The 8 biggest botnets of all time, cybernews. Available at: https://cybernews.com/security/the-8-biggest-botnets-of-all-time/ (Accessed: November 8, 2022).

Smith, B. (2008) ‘A Storm (Worm) Is Brewing’, *Computer (Long Beach, Calif.)*, 41(2), pp. 20–22.

Thanh Vu, S.N., Stege, M., El-Habr, P.I., Bang, J. and Dragoni, N. (2021). A survey on botnets: Incentives, evolution, detection and current trends. *Future Internet*, *13*(8), p.198.

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A. and Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(5).