A Digital Forensics Report Into The Storm Botnet

Isaac Basque-Rice

BSc. (Hons.) Ethical Hacking
Abertay University
Dundee, United Kingdom
1901124@abertay.ac.uk

November 8, 2022
3233 Words

Contents

1 Introduction

In the modern era, reliance on computer networks, and the devices that make them up, has never been higher nor clearer. Naturally, when there are such high levels of collective dependence on individual systems, they become a target for malicious actors seeking to gain money, leverage, or other such things at the expense of others.

A prime example of bad actors using networked devices for their gain is the concept of a malicious botnet, a “collection of computers linked together to perform a specific task” (Fortinet 2022) which, given the wrong person has control of the said botnet, can result in mass email spam, which can be precursors to traditional malware campaigns, Distributed Denial of Service (DDoS) Attacks, cryptocurrency mining schemes, and brute force password cracking attempts (BasuMallick 2022).

According to research conducted by Cognyte CTI Research Group (2022), the computer telephony integration division of Cognyte, a market analysis firm, over 9 million login credentials had been available for sale between 2019 and 2021. Naturally, the real number is likely much higher, given these are simply the ones currently for sale and that could be found by the analysts.

Of particular concern in recent months is the re-emergence of the Storm botnet. This botnet, spread via email spam, was estimated to have spread to up to 50 million devices as of its height in September 2007 (Spiess 2007). At this height, according to some analysts, the botnet had greater computational power than many of the most powerful supercomputers of the time (Gaudin 2007).

Storm’s method of attack and persistence is notably different from other forms of botnets. In most instances, botnets are controlled by a small handful of command-and-control servers, which send out instructions. This is not so with Storm, which takes a distributed peer-to-peer approach, which means there is no central node that, if taken down, would stop the botnet. This, in combination with fast-flux, a DNS evasion technique that constantly shifts DNS resolution within the botnet’s thousands or tens of thousands of resolution servers (Nazario and Holz 2008), severely harmed efforts to prevent the botnet’s spread.

According to a report by Microsoft London, a “relatively new location for Microsoft”, evidence has appeared of a resurgence in the Storm botnet, with suggestions that it may affect Android devices as well as desktop computers. Accordingly, they have hired a Digital Forensics researcher to perform an independent consultation on Storm. This report outlines the steps that researcher will undertake during their work, including, but not limited to, operational costs, data sources, tooling, and so on.

2 Acquisition and Investigation Strategy

At the outset of the investigation, an Acquisition and Investigation Strategy is of the utmost importance. This strategy begins with locating potential data sources, which refers to what sources on the computer network environment could be a resource for the analysis of a potential Storm botnet outbreak. Examples of these include Windows computers and servers, as Storm historically targeted these through malicious executables propagated via email (HelloTech 2016), as well as Android devices, as members of the Microsoft team have been made aware that this particular bot is now propagating through that vector, also.

Many malware developers tend to frequently change strategies, vectors, malware behaviour, and so on, to prevent automated detection. Because of this, a methodology must be produced that is reproducible regardless of the state of the botnet. To this end, the most recent malware sample available to the testers should be ”sandboxed” (placed in a VM with no connection to the wider internet), and run whilst several analysis tools, such as network packet sniffers and process monitors, are also running to gain a greater understanding of what the malware does to the system.

After data sources are identified, a strategic flow to follow must be implemented. This refers to what is essentially a methodology for digital forensic analysis, i.e., what steps are taken, in what order, why are these steps taken, and what is the result. The strategic flow that will be used herein will adhere to the following steps:

- Identification – Before a forensic analysis, it is important to establish firstly *why* forensic analysis is required, as well as what resources will be required, what evidence is present, where it is stored, in what format, and so on.

- Preservation – The evidence collected must be preserved exactly as it was upon discovery *at all times*, this section describes how that is achieved.

- Analysis – Further investigating and examining information/data found within the data sources to build a mental model of what occurred.

- Documentation – To ensure reproducibility and legitimacy, documentation must be produced that shows the steps taken and information found during the investigation

- Presentation – A summary and conclusion of what has been found in layperson’s terms so judgement can be made on the facts as they are.

To this end, what follows is an explanation of what is to happen, i.e. what the strategic flow entails, in this particular case.

2.1 Identification

When it comes to identification, there are typically two crucial categories, these are the identification that an incident has occurred, and the identification of evidence around that incident. Regarding how to specifically identify an incident's occurrence, there are several ways in which this can be achieved. In the abstract, it is possible to identify whether a network or device is infected with a botnet by analysing network traffic to and from suspected infected devices, for example, if a device on the network is being used to propagate the botnet malware through email, a large volume of SMTP traffic and emails will be sent from that device. Other methods of identification include reduced performance on those devices that are infected, unfamiliar processes running or having been run on that device, and modified Windows host files, as well as making use of traditional malware detection techniques (DataDome 2021).

Concerning the evidence of the incident specifically, however, there are naturally several indicators that may be of use when identifying the presence of this particular botnet. The presence of files on-disk named `game0.exe` through `game5.exe` is normally an indicator of compromise by the Storm botnet, as these are the binaries responsible for linking up with other infected devices and "[downloading] additional stages onto the infected system." (Stewart 2007). The malware can also be detected through string analysis, as several values, such as target IP addresses, decryption keys, and P2P peers, are hard-coded into the malware (Stewart 2007).

The National Institute of Standards and Technology's (NIST) 2006 special report into "Integrating Forensic Techniques into Incident Response" (Grance et al. 2006) outlines several crucial data sources that an incident responder and/or digital forensic investigator should use in the identification phase of an investigation. The following is a non-exhaustive list of evidence sources that can be used in a case such as this.

- Intrusion Detection Systems – often used by medium and large organisations (such as Microsoft). This is the "start point for any suspicious activity" (Grance et al. 2006) and can capture and identify suspicious packets

- Security Event Management – Helps analyse log files such as those produced by IDS software

- Network Forensic Analysis Tools – Tools specifically designed to aid in situations such as this, often have the functionality to recreate and visualise past network traffic.

- Packet Sniffers – Such as Wireshark, allow an investigator to monitor internet traffic in real-time as opposed to reconstructions

- Other tools – ISP and DHCP records, logs from firewalls, routers, proxy servers, remote access servers, etc.

2.2 Preservation

The task of preserving the evidence is deceptively complex, as there are several ways with which one could approach this task. The first, and perhaps most obvious method is to create copies of files on disk, particularly those already determined to be associated with the botnet, and then perform a checksum on both the original and copied versions of the associated files, make a note of the resulting hash, and continually check for discrepancies between the two. This is a valid approach, although unfortunately does not go far enough, as there may be both updates to the botnet that introduces newly associated files that the investigator is unaware of, and changes to specific areas of the operating system, such as registry keys, that is not easily isolated into its neat area for analysis.

The alternative, then, is to make a copy, or 'image', of the entire disk, perform the required checksums on that, and then ensure that information is preserved at all times by isolating it from the rest of the network/internet and storing it securely. This approach is more advisable for several reasons, not least because it prevents possibly crucial data that could be presented as evidence from being tampered with or, in the worst-case scenario, being permanently lost, on the original device.

This hash must be collision-resistant, that is, it should not be feasible that two entirely different inputs into the hash function should not result in the same outcome. MD5, a common hashing algorithm, has been found by Wang and Yu (2005) to be cryptographically broken since any arbitrary file, given the fact that specific bytes in specific places are of the correct value, can output any given hash value. This means that should a malicious actor get ahold of the image and have sufficient skill, they would be able to modify the image whilst retaining the md5sum. The authors recommend switching to the SHA-2 family of hashing functions, which have had no collisions to date.

2.3 Analysis

Next comes the Analysis section. Within this section, according to Hoog (2011), it is most important to create a timeline of events before and after, in this case, compromise by the botnet. The tester will start by setting up a honeynet within the network, this honeynet will have a honeywall to prevent further network infection. After this, they will continue by analysing the incoming and outgoing emails over a set period to see whether said emails contain suspicious links, infected attachments, and contents already known to be associated with the botnet. A tool such as Aid4Mail, an email analysis tool with "the highest amount of capability to gather information" as compared to other tools (Devendran, Shahriar, and Clincy 2015), may likely be used.

After this, an analysis of the network will be conducted. The investigator can use 'packet sniffing' tools, which entails them capturing, observing, and analysing data as it moves around the network. The tool that will be used for this will be Wireshark, this tool is the industry standard due to its efficiency, availability, and wider adoption leading to excellent support. The investigator will analyse several protocols, including Ethernet, IP, TCP, HTTP(S), IRC, and, of course, SMTP. The headers in these packets may contain relevant information for the investigation, such as the source and destination, which may be other infected devices, as well as the contents of the packet itself and the flags that were set. This allows the investigator to build a thorough mental model of the botnet and all possibly infected devices on the network.

Finally, the investigator will analyse the logs produced by the firewall, intrusion detection system, operating system, and so on. This is to identify any suspicious activity, such as proxy bypasses, port changes, and so on. By the end of this stage, the analyst should have a fairly comprehensive timeline of events.

2.4 Documentation

Naturally, all of the previous steps must be documented. The full contents of the data retrieved and used in the course of carrying out this work must be recorded, with no stone left unturned, so to speak. At this point, the aforementioned timeline of events will be constructed, as well as the raw data that is of particular note to the investigation, and other artefacts such as the contents of emails, information in data packets sent across or outside of the network, and so on. Of course, if any of this data is of a personal nature (names, home addresses, telephone numbers, passwords, etc) this information will be immediately documented and the relevant parties will be notified, including the Information Commissioner's Office and the individual in question.

It is of the utmost importance, in this stage, that artefacts that indicate any changes between the original Storm botnet and its current iteration be thoroughly documented. This is as essential as it is because an entirely new form of device is being targeted, the android device, and as such the techniques the malware uses are crucial to preventing something like this from reoccurring.

2.5 Presentation

The final step in this investigation will be the presentation stage, wherein the investigator will present their findings to the relevant parties, be they the managerial team of Microsoft London, or, if necessary, law enforcement. This presentation will strive to be as accessible as is reasonably possible for it to be most fully understood, whilst retaining all information about the findings of the investigation.

Clarification should be made of all steps of the attack, from the initial point of access to movement within the network. This is intending to inform the Microsoft London team where any weaknesses and/or vulnerabilities may lie within their internal systems, as well as presenting advice for how to remedy these issues.

3 Discussion and Findings

Once the investigation is complete it is logical and necessary for the investigator to discuss their findings in the report and, of course, propose some solutions to the issues found. This section will assume that the Storm 2022 botnet is fundamentally similar to the original incarnation of the malware.

This section has been divided into two subsections. Firstly, the Implications section, which is concerned with what happens if Storm *is* present on the network, followed then by the Countermeasures section, regarding what can be *done* about the botnet to both prevent and mitigate the worst outcomes.

3.1 Implications

Much has been mentioned in this report regarding what could be done about the Storm botnet if it were to be present on the Microsoft London network, but what are the implications of its presence for the business and staff? Additionally, what are the implications after the investigation described in this report has been carried out?

Firstly, botnet attacks can result in downtime. This, undoubtedly, is one of the biggest concerns any enterprise should have, as the financial impact (as well as the impact on users) of a system being inoperable due to a botnet being present on the network (or at the very least, slower than normal) could be tremendous. According to a study by Lerner (2014), the *average* cost of downtime is $300k per hour, however as Microsoft is a large organisation with a significant number of customers, that number could be significantly, possibly orders of magnitude higher.

Another concern that should be borne in mind is the reputational damage that will no doubt be felt by Microsoft London. When Capital One suffered a data breach in 2019 which resulted in their stock price falling by 6%, with Equifax being down just under 22% on the S&P 500 between its breach and July 2019 (Imbert 2019).

Once the report has been carried out and conclusions have been made regarding how to move forward, naturally, changes will take place. Staff may note an increase in emphasis on security, including changes to the password and email policies, and increased staff awareness training, as the organisation seeks to prevent such an attack from occurring again. Further information on this is found in the following section.

3.2 Countermeasures

3.2.1 Intrusion Detection Systems

An Intrusion Detection System, or IDS, is a specialised piece of network-based tooling used in a multitude of medium to large-scale organisations, such as Microsoft London. The purpose of an IDS is to monitor and detect an intrusion into the network by locating known threats (such as the Storm malware for example) and presenting an alert to the organisation's IT team.

The investigator's recommendation in this instance is to make use of a network-based IDS, which monitors traffic across an entire network. This contrasts with host-based IDS, which detects intrusions into individual systems by detecting possibly malicious activity by monitoring system events. The justification for the use of Network-Based IDS is that the primary detection method for the Storm botnet is through suspicious packets sent across a network.

An example of an IDS that may be used by the organisation is Snort, a free and open source (FOSS) Intrusion Detection and prevention System that can monitor traffic, create logs, analyse protocols, match the content of a packet to already known issues, and much more. The advantage of using a FOSS tool (beyond the fact it comes at no cost to the organisation) is that an audit of the entire codebase is possible, thus ensuring no security issues or bugs, and if they are present an edit can be made.

3.2.2 Staff Training & User Behaviour

In addition to the introduction of an Intrusion Detection System, it is of the utmost importance that the correct amount of emphasis is placed internally on staff training and prevention on an internal user level. As the general reliance on the internet increases, so do the number and variety of threats to businesses. Keeping staff informed of the threats that may be present, including (pertinently to this investigation) possible threats over email, is of the utmost importance.

For this section of the report, staff will be separated into 'users' and 'administrators'. This distinction is made as administrators have both a higher degree of access, and therefore responsibility, for the network, and also because it is assumed (due to the number of users if nothing else) that users are more susceptible to phishing attacks such as the one that Storm uses.

Users can be protected and prevented from making costly mistakes in several ways, including, but not limited to, being reminded quarterly of the importance of basic security practises such as 2-factor authentication and strong passwords, as well as instituting phishing exercises wherein a fake phishing email is sent to staff on a semi-regular basis, and if members of staff click the links within the email provide them with extra security training. All of this is to be done to instil a security mindset at all levels of the organisation.

With regards to Administrators, at the very basic level, it is their responsibility to ensure all systems are up-to-date at all times to prevent the exploitation of any vulnerabilities within any systems on the network. Additionally, it is their responsibility to remain vigilant about any intrusion into the network, learn to use the aforementioned IDS systems well, and be ready to take action in any required areas, including isolating individual machines or accounts, and scanning them for malware.

4 Conclusion

To conclude, this paper aimed to provide Microsoft London with information regarding how a future digital forensics investigation into an attack by the Storm botnet would be carried out to as high and professional a standard as possible. Any prospective investigator will strictly follow a tried-and-true digital forensics methodology that will result in a high-quality report and plan of action for the Microsoft London organisation.

After the description of this methodology, and why each stage is so important, a selection of implications of this botnet attack were explored, including both financial and reputational impact on the organisation. This was followed by countermeasures that could be taken that would result in a net positive security outlook for the organisation.

The most immediate countermeasure that could be implemented is the introduction of an Intrusion Detection and Prevention System, which would have the capacity to alert an administrator or security team of an intrusion and possibly deploy countermeasures to defend against this. The immediacy of this tool is excellent, however ensuring the staff at the organisation are well-trained and are on the lookout, so to speak, for any malicious emails is of the utmost importance, and will serve as the primary line of defence against any future attack.

References

BasuMallick, Chiradeep (May 20, 2022). *What Is Botnet? Definition, Methods, Attack Examples, and Prevention Best Practices for 2022.* Spiceworks. URL: https://www.spiceworks.com/it-security/network-security/articles/what-is-botnet/ (visited on Oct. 15, 2022).

Cognyte CTI Research Group (Mar. 20, 2022). *Botnet Market Statistics.* Cognyte. URL: https://www.cognyte.com/blog/botnet-market-statistics// (visited on Oct. 15, 2022).

DataDome (Feb. 18, 2021). *Botnet Detection: How to Detect & Mitigate Botnets?* DataDome. URL: https://datadome.co/learning-center/how-to-detect-mitigate-botnets/ (visited on Oct. 27, 2022).

Devendran, Vamshee, Hossain Shahriar, and Victor Clincy (Jan. 10, 2015). "A Comparative Study of Email Forensic Tools". In: *Journal of Information Security* 6.2, pp. 111–117. DOI: 10.4236/jis.2015.62012. URL: https://digitalcommons.kennesaw.edu/facpubs/3612.

Fortinet (Mar. 20, 2022). *What Is a Botnet?* Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-botnet (visited on Oct. 15, 2022).

Gaudin, Sharon (Sept. 6, 2007). *Storm Worm Botnet More Powerful Than Top Supercomputers.* URL: https://web.archive.org/web/20071011004946/http://www.informationweek.com/news/showArticle.jhtml?articleID=201804528 (visited on Oct. 18, 2022).

Grance, Timothy et al. (Sept. 1, 2006). "Guide to Integrating Forensic Techniques into Incident Response". In: *NIST.* URL: https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response (visited on Oct. 28, 2022).

HelloTech (Sept. 23, 2016). *Storm Worm – Malware Information, Detection and Removal.* The Plug - HelloTech. URL: https://www.hellotech.com/blog/storm-worm-malware (visited on Oct. 25, 2022).

Hoog, Andrew (June 16, 2011). "A Geek's Guide to Digital Forensics, or How i Learned to Stop Worrying and Love the Hex Editor". URL: https://www.youtube.com/watch?v=rPd-HiEvhhw (visited on Oct. 31, 2022).

Imbert, Fred (July 30, 2019). "Capital One Shares Dive after Data Breach Affecting 100 Million". In: *CNBC.* URL: https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html (visited on Nov. 6, 2022).

Lerner, Andrew (July 16, 2014). *The Cost of Downtime.* Andrew Lerner. URL: https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/ (visited on Nov. 6, 2022).

Nazario, Jose and Thorsten Holz (Oct. 2008). “As the Net Churns: Fast-flux Botnet Observations”. In: *2008 3rd International Conference on Malicious and Unwanted Software (MALWARE)*. 2008 3rd International Conference on Malicious and Unwanted Software (MALWARE), pp. 24–31. DOI: 10.1109/MALWARE.2008.4690854.

Scanlon, Mark (Dec. 9, 2017). *Study of Peer-to-Peer Network Based Cybercrime Investigation: Application on Botnet Technologies*. DOI: 10.48550/arXiv.1712.03455. arXiv: 1712.03455 [cs]. URL: http://arxiv.org/abs/1712.03455 (visited on Oct. 24, 2022).

Spiess, Kevin (Sept. 7, 2007). *Worm 'Storm' Gathers Strength*. Neoseeker. URL: https://www.neoseeker.com/news/7103-worm-storm-gathers-strength/ (visited on Oct. 18, 2022).

Stewart, Joe (Feb. 7, 2007). *Storm Worm DDoS Attack Threat Analysis & Report*. Secureworks. URL: https://www.secureworks.com/research/storm-worm (visited on Oct. 27, 2022).

Wang, Xiaoyun and Hongbo Yu (2005). “How to Break MD5 and Other Hash Functions”. In: *Advances in Cryptology – EUROCRYPT 2005*. Ed. by Ronald Cramer. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 19–35. ISBN: 978-3-540-32055-5. DOI: 10.1007/11426639_2.