Abertay University®

Advanced Digital Forensics: Unit 1 - Research Report

A digital forensic methodology proposed for carrying out an investigation into the 'Storm Botnet' scenario.

Marc Geggan

CMP416: Advanced Digital Forensics

2022/23

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

Contents

1 INTRODUCTION

1.1 BACKGROUND

A botnet ("robot network") is an interconnected network of infected computers, mobile devices, or IoT devices. These devices are infected with malware that allows an individual threat actor, known as a 'bot-herder', to send commands from a remote central location to every infected device on the network with the purpose of simultaneously carrying out a coordinated attack. *(Paloalto Networks, 2019).* The bots serve as a tool to automate mass directed attacks, such as data theft, distributed denial of service (DDoS) attacks, malware distribution, and crypto mining *(Kaspersky, 2020).*

A threat actor will spread their botnet malware using various techniques such as social engineering, spam email, ad pop-ups, and malicious downloads. Once a target has downloaded this seemingly harmless software their device becomes infected. Some botnets can also self-propagate and scan the internet for network enabled devices to automatically infect through known vulnerabilities or default passwords *(Jolera, 2019)*.

Botnet networks can take up different structures, designed to give the bot-herder as much control as possible. The two main botnet models are called client-server (C&C), and peer-to-peer (P2P). The C&C model is a centralized botnet model that uses one or more servers to communicate to infected devices (*See figure 1)*.

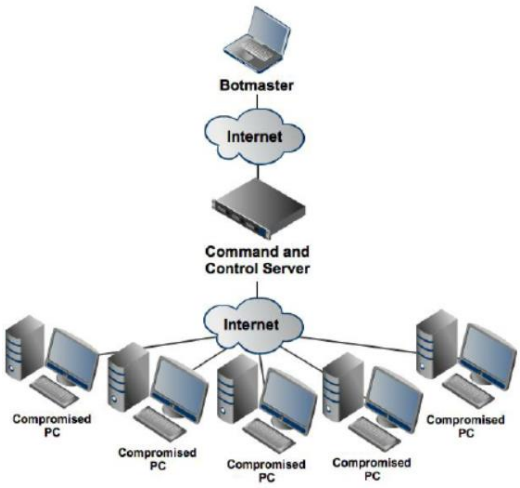

Figure 1: *Typical Client-Server Botnet Command and Control Topology. (Scanlon et al., 2012).*

A P2P botnet model is decentralized, meaning there is no central command-and-control server. The bots are connected topologically and act as both the client and server *(see figure 2).* When a bot receives a command, it is executed and forwarded to any other bots it is aware of. This means a bot-herder can connect to the infected network, push a command out, and disconnect whilst the command propagates itself throughout the network *(Wang et al., 2010)*.

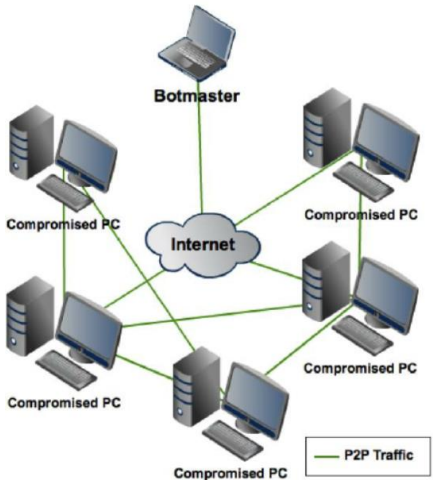

Figure 2: *Typical Peer-to-Peer Botnet Command and Control Topology. (Scanlon et al., 2012).*

The storm botnet of 2007 was the most wide-spread P2P bot found on the internet. It came in the form of a trojan-horse malware, presenting itself as a downloadable file sent via spam email campaigns. Once downloaded it turned the infected device into a bot and automated attacks such as DDoS and spam campaigns. The storm malware infected an estimated one million or more devices in its prime, and targeted machines running certain versions of windows.

1.2 AIM

This report is based on a given scenario stating that a modernized version of the storm botnet has resurfaced. It attacks the newest versions of windows, with evidence of it affecting both PC's and Android smartphones through local networks. Microsoft London has requested an independent consultation into the matter, requiring information on the digital forensic procedure, detecting malware, and possible countermeasures.

This report aims to fulfil the request of Microsoft London as stated above and propose an appropriate methodology for analyzing the 2022 storm worm botnet. An overview of the methodology, or strategic flow, being proposed is as follows:

1. Identification
2. Preservation
3. Analysis
4. Documentation
5. Presentation

The following sections within the report will go into more detail of each stage within the forensic methodology, providing appropriate methods, tools, reasoning, and countermeasures for the 2022 Storm botnet investigation.

2 ACQUISITION AND INVESTIGATION STRATEGY

A methodology must be followed to ensure thorough forensic investigation into Microsoft London's network for evidence of the Storm botnet. This methodology and concise description for each stage is as follows:

Identification
The first stage of the investigation. The forensic investigator will observe the current situation and identify the devices and resources believed to contain data that will be part of the investigation. These devices of interest would then be seized and isolated, and any networks secured.

Preservation
After devices of interest have been secured by the investigator, data will be preserved. Forensic techniques discussed later in the report will be used to extract data relevant to the investigation and stored securely to ensure accuracy and credibility.

Analysis
At this stage, all devices involved have been identified and isolated, and data of interest has been duplicated and stored securely. The investigator will now examine all the data using a multitude of different forensic techniques. The analysis techniques used will vary depending on the investigation and the specific steps proposed here will be discussed in the next section of the report.

Documentation
After extensive analysis of data, it is of upmost importance that the results and findings are properly documented. This allows for future examination, developing reports, activity timelines, and provide an overall visual of the investigation.

Presentation
After the investigation is complete, all the data and results that have been documented will be formulated into a report and presented to the client – Microsoft London.

2.1 STRATEGIC FLOW

2.1.1 Identification

The brief provided from the client explains they require a potential investigation into a new variant of the Storm botnet. This new variation is believed to affect both Windows PC's and Android smartphones through local networks. The client wishes to investigate if they have already been affected by the new variant and any potential devices and data sources of interest. This first stage of the investigation aims to identify these devices of interest, seize them, and store them securely.
To identify if any of the devices within the Microsoft London network have been infected with Storm malware, there are multiple tools and techniques that can be used. Due to the botnet malware propagating through local network traffic, the investigator will focus heavily on network packets, port analysis, and unusual network activity.

Firstly, the investigator will look at network packets and traffic. This is done using Wireshark, an open-source free 'industry standard' network packet capture and analyzer tool. Once set up on the network, it will capture all packets it can find in real time and allow the investigator to filter through results to visualize relevant data. The data recorded can be used to identify malicious activities and compared to the previous Storm botnets known methods of communication. Wireshark will be run and used against both PC and Android phone network traffic.

The original Storm botnet malware, once executed on a target machine, was known to install an encoded configuration file with information about other peers on the network and their IP addresses / port numbers. This configuration file opens ports to allow it to join the P2P network *(Holz, et al., n.d.)* NMAP is a free open-source tool used for network discovery and security auditing. It can be used to scan for all the open ports on devices by using the -p command. The investigator will scan devices ports and compare results to that of known ports used by the Storm botnet to communicate with the P2P network. If the client uses web proxies, there may also be activity logs of incoming and outgoing packets through ports that can be analyzed.

Intrusion detection systems (IDS) are a device or software that can be installed to monitor network traffic for malicious activity or policy violations. The host will set various rules and create a 'normal' baseline for it to work from. Anything deemed malicious will be logged in its event management system so a security analyst can view it. Although they don't defend against the attack, the logs can be useful in determining infection. IDSs are common and if Microsoft London has implemented one, the logs will be used to identify signs of infected devices.

2.1.2 Preservation

After devices of interest have been established, the investigator must start preserving all the data from the devices. The technique to do this will vary depending on the type of device being preserved, however they all follow the same principle of extracting an image or copy of data from the device. Before taking the devices away from the scene it will be considered whether it is safe to unplug the devices from the power and secure the network or not. Next, the devices data will be extracted for analysis. For the Windows PC's, a disk-to-disk image can be taken of the device by mounting it to the forensic laptop running CAINE live operating system. This is a free industry standard operating system for digital forensics. Within CAINE there is a tool called FTKImager, that will be used to take a bit for bit copy of the target machine and generate a hash checksum to ensure data integrity. This checksum will be generated in MD5 or SHA1.

The brief also explains that the new malware may infect Android mobile devices. MVT (Mobile Verification Toolkit) is a tool designed specifically for mobile forensics and detecting signs of compromise. It is free and can be found as a python package on GitHub. Command line commands will be used to mount the filesystem of the mobile and an image will be taken of it.

After images of both PC's and Android devices have been taken, the devices can be stored securely, disconnected from networks and away from tampering, and the data extracted can now be analyzed.

2.1.3 Analysis

After the data has been extracted from all areas of interest it can be forensically analysed within the investigator's lab. Firstly, the investigator will examine the captured network data from Wireshark and NMAP. The captured packets will be filtered for known Storm botnet communication methods such as

SMTP traffic and any unusual open TCP/UDP ports from the scan will be observed. Next, malicious activity logs will be monitored from intrusion detection systems if present on the network.
If any of the tests completed so far have uncovered concerning evidence, more granular analysis of the device will be carried out to test for botnet malware. This can be done by analyzing the filesystem images taken from the devices and stored on the forensic workstation. It was noted from the old Storm botnet that it would install configuration files on infected devices, so the investigator would start file carving techniques to look for evidence of these files that connect it to the P2P network.
As the original Storm botnet was introduced to local networks through spam emails, it may be beneficial to examine some email accounts. Spam-trap accounts from the time of the original Storm spam campaign can be compared to staff emails for similarities. This may not be as effective as network analysis, the new Storm botnet may use different techniques, however if it is built on top of the old version its malware may still be sent via spam campaigns.

2.1.4 Documentation

Contemporaneous notes will be taken throughout the forensic investigation and will cover the full record of actions taken and results produced. Many guidelines have been published on best practice when it comes to documenting a digital forensic investigation, and the investigation into the Storm botnet intends to comply with these best practices to ensure it would stand in a court of law and provide effective information. The main guidelines that will be followed when documenting information come from several leading digital forensic organizations:

- ACPO – Association of Police Chief Officers
- ENFSI - European Network of Forensic Science Institutes
- NIST – National Institute of Standards and Technology

These guidelines all explain the importance of taking detailed notes throughout every stage of the investigation. The ACPO report titled *'Good Practice Guide for Digital Evidence*' states that data reporting Is the ultimate product from the investigation and the documentation should be preserved so a full report may be drafted from it. Principle 3 within the document explains that all processes of the investigation should be documented and preserved, and an independent third party should be able to reproduce the investigation *(Williams, 2011)*. It also gives a guide on specific important records to keep, which will be followed meticulously throughout the investigation. The ENFSI published a document called *'Best Practice Manual for the Forensic Examination of Digital Technology'* stating the importance of documenting tools. It goes on to talk about the use of two or more tools with the same function and the importance of documenting both sets of results within the notes. It also suggests backing up the use of tools with specific reasoning regarding their functionality and relevance to the investigation *(ENFSI, 2015).*
The forensic investigation will follow the information and guidelines provided by these professional organizations and the notes taken will be stored securely. The documentation will also be accurate and designed so that a third-party analyst may recreate the whole investigation from start to finish.

2.1.5 Presentation

The final stage of the forensic investigation will be presenting all findings to the client – Microsoft London. It is imperative that the reporting is completed correctly as the outcome of the investigation and details within the report will be used to make potentially very expensive and drastic changes to company

operations. The deliverable will contain both technical and non-technical reports based on the previous four stages on the investigation, a best practice when presenting information to multiple audiences of different technical backgrounds.

The technical report, aimed at IT professionals within the company, will document detailed low-level technical information on how the investigation was carried out, and any data dumps, logs, port scans, packet analysis results, or other significant information will be attached. The detailed findings are required to provide credible evidence of the investigation and ensure that if the research was used in legal proceedings, it would stand in accordance with the court of law. This information may not be as important to other parties involved and so a non-technical report will also be produced. This report will still contain a timeline of events and high-level investigation findings, but will be aimed towards the impact on business, likelihood of infection, suggested countermeasures and less technical details. This style of report is found most useful to project managers, directors, and CEO's.

3 DISCUSSION AND FINDINGS

3.1 COUNTERMEASURES

Regardless of whether the devices within Microsoft London office were infected, it is always best practice to implement some countermeasures to defend from malware. This section will provide some countermeasures regarding the new variant of Storm botnet malware and similar issues in the future. Firstly, if not already implemented, an intrusion detection system should be deployed. Specific rules should be set that monitor high volumes of network traffic at unusual times and it should be set up to report these malicious activities to activity logs. The IDS called snort is a well-known IDS software that can be implemented to the network for free, and extras can be added on with a business starting cost of $399 per sensor. A free alternative to this could be OSSEC by TrendMicro, an open-source IDS.

Staff cyber security training also needs to be implemented regularly. Making staff aware of this threat and what to look out for may reduce the chance of the malware ever getting onto the local network. Phishing campaigns should be run regularly to keep staff up to date on threats.

A zero-trust policy can also be implemented within the office. This is where only fully verified devices and software can be accessed by staff and over time new verified devices can be trusted. This makes it harder for malware to traverse through the network as staff may not be allowed to download attachments or autorun software.

Staff endpoint devices such as mobile phones can be a big security risk. Endpoint detection and response (EDR) tools can be implemented to the network that uses machine-learning and threat detection techniques to detect threats by monitoring internal and external traffic of endpoint devices.

Implementing a honeypot to the network can also be useful in identifying malware types trying to infect devices. This is where a decoy device is set up on the network and logs all connection attempts and types to be analysed against known attack methods. Using honeypots, much more can be learned about the new variant of the Storm botnet such as how it operates, what it looks for, and how it spreads.

3.2 IMPLICATIONS OF BOTNET

Failing to implement countermeasures for this new variant and future attacks could have severe implications, especially if Microsoft did eventually become infected with this botnet malware. Firstly, Microsoft would experience major reputational damage due to the loss of partnership interest and customers losing confidence in Microsoft products. This damage to reputation will also bring major Financial damage. Fines may be imposed by governing bodies for failing to act on cyber security threats, putting customer and staff data at risk. The downtime of staff machines and company networks may also result in financial loss. If the network needs rebuilt or repaired due to the potential damage of the malware, staff will not have access to devices to complete projects and new devices may cost the company. It was also discovered that the previous Storm botnet was used for credential harvesting, this means that staff data may be stolen and used for illicit activities. Rootkits and backdoors can be installed on systems making it easier for hackers to gain access to customer and staff data.

4 CONCLUSIONS

4.1 CONCLUSIONS

To conclude, the Storm botnet malware poses a real danger to networks. The P2P botnet in its prime of 2007 infected an estimated one million plus devices and would hijack them to be used for illegal activities. Although the extent of the new version has not yet been discovered, investigators can use data from past research to help design a methodology for detecting and mitigating the new variation. This report has successfully provided a proposed methodology for conducting a digital forensic investigation within the Microsoft network. Starting with identifying possible target devices through network analysis, the methodology then provides techniques for extracting and storing the data, and then moves into an analysis of PC and Android devices for possible evidence of infection. Per request of the client, some information has been provided on further granular identification and countermeasures help detect and defend from the new variation and similar attacks in the future. Finally, the investigator provided details on the implications Microsoft may face if they were infected with the new variant botnet, such as reputational damage and financial loss. Nevertheless, with an accurate and professional forensic investigation followed up with suggested countermeasures, Microsoft will significantly reduce their chance of becoming infected with this new variant.

REFERENCES

Paloaltonetworks.com. (2019). *What is a Botnet? - Palo Alto Networks*. [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet. [Accessed 3 Nov. 2022].

www.kaspersky.co.uk. (2020). *What is a Botnet?* [online] Available at: https://www.kaspersky.co.uk/resource-center/threats/botnet-attacks. [Accessed 3 Nov. 2022].

Jolera (2019). *How Botnets Infect Your Computers*. [online] Jolera. Available at: https://www.jolera.com/how-botnets-infect-your-computers [Accessed 3 Nov. 2022].

Scanlon, M., Kechadi, T., 2012. Peer-to-Peer Botnet Investigation: A Review. pp. 231–238. https://doi.org/10.1007/978-94-007-5064-7_33

Wang, P., Aslam, B., Zou, C.C., 2010. Peer-to-Peer Botnets, in: Stavroulakis, P., Stamp, M. (Eds.), Handbook of Information and Communication Security. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 335–350. https://doi.org/10.1007/978-3-642-04117-4_18

robAdmin (2019). *Digital Forensics Documentation - Contemporaneous Notes Required*. [online] Forensic Notes. Available at: https://www.forensicnotes.com/digital-forensics-documentation-contemporaneous-notes-required/

Williams, J. (2011). *ACPO Good Practice Guide for Digital Evidence*. [online] Available at: https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.

Best Practice Manual for the Forensic Examination of Digital Technology. (2015). [online] Available at: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

NATIONAL COMMISSION ON FORENSIC SCIENCE Critical Steps to Accreditation. (2016). [online] Available at: https://www.ascld.org/wp-content/uploads/2016/03/Final-Draft-Views-Document-on-Critical-Steps-to-Accreditation.pdf

Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F., n.d. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm 9.