Abertay University

Research Report

Discussing the entire process of undertaking a forensic investigation

Patrick Collins

CMP416 – Advanced Digital Forensics

BSc Ethical Hacking Year 4

2022/23

Abstract

In 2007 a new worm threat called Storm surfaced that mass spammed millions of emails with catchy news titles to get users to open the email which turned into a botnet. Storm was one of the first botnets that was connected peer-to-peer. It targeted the Windows operating system as it was a very popular with millions of users. It was a trojan virus and worm that spread to other email addresses and can receive commands from a remote server. However, in 2022 Storm is back in full force and has been modified changing how it functions to modernise it.

On request of Microsoft London a forensic investigator has given an example of An Acquisition and Investigation strategy that contains the procedure that can be followed to investigate the Storm 2022 botnet in the Microsoft London network.

If Microsoft decides to continue, the investigator would be pleased to carry out a full forensic investigation on the London network using the strategy discussed in this research report.

Table of Contents

Introduction

In 2007 a new worm threat surfaced that mass spammed millions of emails with catchy news titles to get users to open the email (Spiess, 2007). For example, one of the email subjects included “230 dead as Storm batters Europe” (Mikkelson, 2013). This is how the Storm botnet got its name. It targeted the Windows operating system as it was a very popular operating system with millions of users.

The exact worm the Storm botnet had maliciously embedded in the emails is called “W32/Waledac.A” (F-Secure, n.d). It is a trojan virus and worm that spreads to other email addresses that can receive commands from a remote server. This is how the botnet was controlled back in 2007. Once a user clicked on the email attachment it automatically downloaded the worm and caused the machine to turn into a bot (F-Secure, n.d).

Storm was one of the first botnets that was connected peer-to-peer. This means that it connected to other machines to form network to attack the same target in sync. It was also the first botnets to be controlled by several different servers. Although the large scale of this operation, it was shut down in 2008 just a year after it was released. This happened due to some the servers being shut down, halting it’s operation as there was no way to effectively control the botnet anymore. Another major factor is that Microsoft released a malicious software removal tool that claimed to remove 500,000 of affected Storm botnet machines (Keizer, 2008). The botnet which had millions of computers at its disposal only had around 85,000 when it was being shut down (Keizer, 2008).

However, in 2022 Storm is back in full force and has been modified changing how it functions to modernise it. Now, the botnet targets the latest versions of Windows with evidence it’s also harming PC and Android Smartphone devices. Storm 2022 does this by infecting computers through the local network. This could be achieved through network-based attacks by exploiting vulnerabilities to spread.

Due to this recent development Microsoft London has tasked a researcher to do an independent consultation on the situation. It’s the aim of the investigation to give Microsoft a better understanding of how a forensics investigation would be undertaken. After, the researcher may be hired to conduct a full investigation after successful consultation.

Microsoft London are interested to know what data sources would be useful for detection and response, and operational trade-offs. Such as high expenditure. Knowing where to place detection plans will help create countermeasures for the botnet that could affect the London office’s network. They also want to know the likelihood of finding and shutting down the new Storm botnet and how to detect/stop similar attacks in the future.

The report is structured using an Acquisition and Investigation strategy. This is to successfully cover all key aspects of a digital intruder investigation by the researcher. After the investigation the results will be discussed, and findings presented to Microsoft London. Countermeasures will then be provided to help secure their network from Storm and the possibility of shutting down the new botnet.

Acquisition and Investigation strategy

Identification

The purpose of this investigation is to give Microsoft a better understanding of a digital intruder investigation. The main aim is to identify how to implement detection and response measures to stop the Storm 2022 botnet and secure the Microsoft London network.

To do this a couple of resources are needed:

- Wireshark
- Snort
- Ngrep
- TCPdump
- Event logs

Wireshark will analyse network traffic to detect how the botnet behaves and communicates with other computers. The botnet spreads through local computers in the network so it would be necessary to identify how exactly it is doing this on the network layer.

Snort will be used to detect when the botnet affects a system on the network. This can be achieved through implementing rules to set off the alarm if an attack is happening. Finally, once the measures have been identified they will have to be implemented to secure the network from any attacks from Storm in the future.

Ngrep analyses network traffic which will be useful to analyse packets in the network. TCPdump is very similar to Ngrep, making it easier to analyse packets captured from either Wireshark or Ngrep. Using these tools allows regular expressions to be used, making it far more efficient to find information about the network. Such as IP addresses or protocols.

Event logs will provide detailed timing of events that occurring on the network and systems. This information is invaluable as it will provide a timeline of the attack and better understand where to deploy resources.

Preservation

In the event of a botnet attack on the network the investigator will preserve the affected systems to collect data for analysis later. For example, if a machine is discovered to have the botnet on it the affected system will be disconnected from the network to preserve the state. From here it's safe to collect data in a controlled environment on the botnet functions and stopping the spread. Also, a bit-to-bit copy of the hard drives will be made before carrying out analysis as to preserve it's state (IGI, n.d.).

Furthermore, at this stage the tools identified will be run. The data collected here from Wireshark and Snort will provide a good amount of data to be analysed for the next stage. Preserving the data is vital to understand the scale of the attack and understand what exactly to investigate.

Analysis

After identifying the data to collect and preserving it the next step in the investigation is to analyse to understand the attack. In this scenario we are attempting to understand how the new Storm botnet functions. A great start would be to look for key features of how the previous botnet functioned in the newer 2022 version. The attackers may still be using the previous methods.

Previous methods to look out for:

- Search for the affected machines connecting to a server in the captured packets.
- Heavy traffic going out from a machine which could indicate the machine is being used for an attack.
- Email communications containing the Storm 2022 botnet file which was then downloaded by a user in the network.

These previous methods and data captured on the network can be analysed by using many tools which will aid the researcher in the forensic investigation.

The PCAP files captured during preservation stage can be analysed in Wireshark itself. Many filters can be applied to filter by IP address, protocol, port number and much more. This makes it far more efficient to discover important information. Furthermore, Tshark can be used to access certain plugin features not available to Wireshark GUI. Tshark is a command line version of Wireshark with these extra plugins. During the forensic investigation these plugins may be used to further aid the investigator in the analysis stage. Email communications can be filtered by SMTP protocol making it easier to identify spam email to users on the network.

Whilst a detection tool, Snort can also be used for analysis. An input file can be loaded into Snort which will display all the packets and a breakdown by protocol. For example, it may show the number of packets containing TCP/UDP traffic. The input can be filtered to only display packets from these protocols. This will speed up the forensic investigation.

Ngrep can be used to filter packets that contain a certain phrase. In this scenario it would be beneficial to filter for the name “Storm”. Any packet captured that contains this will then be displayed to be analysed. A timeline can then be created based on the returned IP addresses, date/time and the ports used. The first instance to last instance of the Storm spreading through the network will be identifiable.

TCPdump is used to filter network traffic from many protocol headers (IP, TCP,UDP, Ethernet Frame). It is a very in-depth analysis tool to find information such as IP header length, displaying packets with certain flags and IP options set.

Alongside the tools to analyse network traffic, many sources of data can be looked upon to understand the threat better. The event logs used in Windows operating system can be analysed to find the timeline of attack which will help the investigator paint a picture of the attack and when it occurred. Moreover, a firewall and router’s logs provide the investigator with a fantastic resource to analyse the traffic that has come through the network and what events have been flagged.

Documentation

In this stage the objective is to capture as much information as possible about the crime scene. This is done by photographing and sketching the scene. The initial investigation is complete and it's now time to gather the results to present to the judge and jury/Microsoft.

The report will have concrete evidence that there is evidence of Storm on the network, and which machines on the network have fell victim to the botnet. How the attack occurred will also be included.

Presentation

In the final stage of a forensic investigation the investigator will make an organised report to summarise the findings about the case. The report is normally presented to a judge and jury and will be designed for this audience accordingly. In this case the report will be given to Microsoft London. It will contain facts about the investigation and the results. When the attacker(s) responsible for creation and deployment of the botnet on the networks are discovered and tracked down this information can be the evidence used to incriminate them for their crimes.

As discovered in the analysis stage the presentation will contain all affected systems, timeline of attack, spam email communications to users, how the botnet spread and got into the network. The report will contain an explanation of the results for Microsoft London to understand the outcome of the forensic investigation.

Discussion and Findings

General Discussion

Many data sources have been identified that can be investigated in the London network for traces of the Storm network. The threat of the previous version of Storm has been discussed and the power the newer version could hold. A forensic investigation strategy explains the steps needed to effectively cover all elements of this scenario.

Countermeasures - Detect and Stop Similar Attacks in the Future.

NIDS/IPS

A Network Intrusion Detection System (NIDS) and a Host-Based Intrusion Detection System could be deployed on the London Network. NIDS will intercept all traffic in the network to look out for large communication between systems on the network which could be the botnet replicating through a worm. Once the NIDS detects suspicious traffic, an Intrusion Prevention System (IPS) could be deployed to handle these threats. The IPS can automatically block suspicious traffic and emails to staff members.

Network Traffic Analysis

Continuously monitoring all network traffic for suspicious activity on the Microsoft London network will keep the network secure from the botnet. Any suspicious activity will be immediately discovered, reported, investigated and then secured. The botnet will not get a strong hold on the network if it is discovered early through analysis. The analysis can be done through the many tools discussed in the Analysis stage of the forensic investigation strategy.

Honeypots

A fantastic countermeasure against a malicious attacker is to have honeypots set up on the London network. A honeypot will effectively trap the botnet by acting as a valuable target that is vulnerable. Once the Storm botnet attempts to compromise the network, it will only attack and compromise this server. Once the server has been compromised the threat is secured and the company will be alerted to the threat with no damage done to important systems.

Using a honeypot will allow the methods the attacker is using to be discovered safely. The methods that Storm 2022 botnet will be using to spread will be identifiable and then specific countermeasures can be implemented for the updated version of Storm.

Staff training against phishing emails

To prevent the botnet from getting access to the London network, staff should be trained to spot a Phishing email attempt such as the ones discussed previously. This will stop the Storm 2022 botnet at its root cause. When a staff member is faced with

a suspicious email being spammed or a suspicious website/advert the training will help identify that this is an attempt to compromise the London network and should be ignored. Most importantly the compromise attempt should be reported.

Backup data

Regular backups of data on the London network should be carried out. If the botnet successfully bypasses the countermeasures put in place to prevent it, full data backups provide an easy means to rid the infected machine of the botnet virus. A simple fresh install to the affected systems and the botnet will be removed from the London network.

Keep software and virus definitions up to date

A successful botnet compromising a system is mainly due to vulnerabilities existing in the operating system or out of date software/anti-virus definitions. Ensure that all software on the system is continuously checked for new updates fixing these vulnerabilities and any new anti-virus definitions such as in Windows Defender.

Android botnet prevention

The newer version of Storm is thought to be targeting Android smartphone devices. We can effectively predict how this would be achieved by looking at previous attempts at botnets attacking Smartphone devices. The same vulnerabilities and exploits may be used in order to spread Storm 2022.

Last year in 2021 an android botnet called “Matryosh” spread to android devices due to the Android Debug Bridge(ADB) (Arntz, 2021). Devices that had this debugging feature enabled opened port 5555 on their device. However, if this port is open over the internet for remote access malicious attackers can use this port as well. This is a very recent attack method making it very possible to be used by Storm 2022.

The countermeasure for this is to simply check if port 5555 is in use, and if so, disable debugging mode on the android device in the settings (Arntz, 2021). Then check if port 5555 is disabled and the device is not remotely accessible from the internet.

Shutting Down the New Storm 2022 Botnet

The previous version of Storm made it very difficult to track it down and research how it functioned due to the defence measures the botnet had implemented. If a researcher attempted to investigate the botnet, a DDOS attack was sent immediately back to the researcher preventing investigation and a warning to not continue with their investigation (Keizer, 2007).

This will make it difficult to research how Storm 2022 functions as the same, or even better, protection measures could be in place. Research can still be carried out but it’s a good idea to be wary of the defence measures it could have in place. A controlled environment to research would be needed.

The solution to the previous botnet version was to have malicious removal tools for the affected systems. The same can be attempted across the Windows operating system once we get a better understanding of how it functions. Furthermore, the botnet eventually died out once the servers began to be shut down. If Storm 2022 uses a form of command and control (C&C) servers then this would be the target to kill the botnet in its tracks.

Conclusion

Storm was a very aggressive botnet with well planned out protection measures to prevent security researchers from discovering and stopping the botnet. News of Storm coming back as a modernised version should be taken very seriously as the first iteration took over the internet affecting millions of systems.

A strategy to investigate Storm 2022 has been provided and discussed. However, it would be beneficial to get details on the London network as it’s currently theoretical. If Microsoft decides to continue, the investigator would be pleased to carry out a full forensic investigation on the London network using the strategy discussed in this research report.

References

Spiess, K. (2007) *Worm 'storm' gathers strength*, *Neoseeker*. Available at: https://www.neoseeker.com/news/7103-worm-storm-gathers-strength/ [Accessed November 3, 2022].

Mikkelson, D. (2013) *Valentine's Day worm*, *Snopes*. Snopes.com. Available at: https://www.snopes.com/fact-check/valentines-day-worm/ [Accessed November 3, 2022].

F-Secure (no date) *Email-worm:W32/waledac.a*, *Email-Worm:W32/Waledac.A Description | F-Secure Labs*. Available at: https://www.f-secure.com/v-descs/email-worm_w32_waledac_a.shtml [Accessed November 3, 2022].

Keizer, G. (2008) *Microsoft: We took out storm botnet*, *Computerworld*. Computerworld. Available at: https://www.computerworld.com/article/2536783/microsoft--we-took-out-storm-botnet.html [Accessed: November 4, 2022].

Keizer, G. (2008). Top botnets control 1M hijacked computers, *ComputerWorld*, 9 April. [online] Available at: https://www.computerworld.com/article/2536378/top-botnets-control-1m-hijacked-computers.html [Accessed November 3, 2022].

IGI, (no date), What is bit stream image, IGI Global. Available at: https://www.igi-global.com/dictionary/bit-stream-image/44363 [Accessed November 9, 2022].

Arntz, P. (2021) *Android devices caught in matryosh botnet: Malwarebytes labs*, *Malwarebytes*. Available at: https://www.malwarebytes.com/blog/news/2021/02/android-devices-caught-in-matryosh-botnet [Accessed November 9, 2022].

Keizer, G. (2007) *'we're not scared' of storm, say researchers*, *Computerworld*. Computerworld. Available at: https://www.computerworld.com/article/2539571/-we-re-not-scared--of-storm--say-researchers.html [Accessed November 10, 2022].