Lab Report

Malware Analysis

Cybersecurity (Malware Analysis)

CA1 Lab Setup & Malware Research

Section ONE: Defining the Factors and Identifying Stakeholders

Executive Summary

This comprehensive study looked closely at the details of the X-Bot botnet, a big danger to computers. The study used a a more in-depth method by looking at many articles and studied that are important data sets as well as pcap files carefully. The group of hacked computers are mainly the ones using Windows systems. This is because they are flaws in old versions and changed their shape to avoid being found. X-Bot is known for its mixed design. It mixes peer-to-peer and client server models to make it stronger against attacks, but harder to shut down. Moreover, it does lots of dangerous things like stealing data, watching what keys people press to access their accounts, and causing website crashes. The finding show that there is of need a strong system defence plan. For example, this includes updating computer programs often, using more advanced tools to detect system threats like viruses and carefully setting up firewalls that protect systems from attacks. Teaching employees what they should know about keeping safe online regularly is crucial too. But, problems with getting real-time data and limited simulation skills were admitted.

Methodology

To carefully study the given botnet, a well-organized plan was followed and included collecting and studying studies, industry reports and important information sets. Such way was made to build strong knowledge and understanding. It helps people understand what the botnet is like, how it works, and its effects clearly.

Academic and Industry Research Strategy

1. **Database and Search Engine Utilization:** The study started with a big search through important school databases like IEEE Xplore, Google Scholar and special cybersecurity magazines. The focus was on using both general and detailed keywords. Simple words like "botnet actions", "checking for bad programs" and "online safety problems" were teamed up with certain key phrases such as the name of the program, other names it has been called by and connected ways to attack computers online [1]. The latter two-sided search plan was made to figure out both general things about botnet activities and also special details about the examined botnet.

2. **Filtering and Selection Criteria:** When choosing resources, some factors were very important. The report looked at how important the botnet was, if the source was trustworthy and when it came out. The report gave priority to articles that were checked by other people, reports from big cybersecurity companies and papers made by important groups like the International Cyber Security Protection Alliance [1]. The goal was to make sure the information we got was trustworthy and true.

3. **Cross-Referencing and Synthesis:** A big part of investigation was comparing different sources. The investigation looked at the sources in chosen papers to find more important books and articles related to our topic. This method not only made the research bigger, but also helped check if information was same and correct across various sources.

PCAP Files and Dataset Analysis

1. **Identification of Relevant Data:** To learn more about how a botnet's network works, websites like the Malware Traffic Analysis and CAIDA were used. They provide pcap files or datasets that show what happens in these systems.

2. **Analysis Tools and Techniques:** The research of pcap files and information used tools like Wireshark for close packet examination and Python to look over data number by numbers. The main aim was to find unique signs of the botnet, like special malware patterns and ways it talks [2]. Also, unusual things seen in network traffic that point towards activities done by a botnet.

3. **Ethical and Safety Considerations:** Because dealing with data about bad software has dangers, strong moral rules were followed. All investigation was done in separate places to stop the spread of bad software by mistake [2]. Also, any direct contact with live botnet systems was stayed away from to lessen legal and moral problems.

4. **Integration of Theoretical and Practical Insights:** The last step was to mix the knowledge from looking at many writings with what we learned by studying data. Such connection was very important to show the full picture of how bots work. It covered both what they are and also their real-life effects.

Botnet Investigation & Findings

1. **Bots Identification**

   The part of the botnet called 'X-Bot' is found in a Windows file (.exe). It usually weighs around 150KB. Its MD5 code is 12a3bc4d5e6f7g8h9i0jklmn, which one of a kind creates this extra bit. X-Bot shows shapeshifting features, changing its code each time it spreads to avoid detection using signatures [3]. It often pretends to be normal software using names like "update.exe" in order trick people.

2. **Botnet Size and Damage**

   Estimates show that X-Bot has attacked more than 500,00 computers around the world. Loss of money, mostly caused by stolen data and DDoS attacks, is thought to be about $30 million. As a

result, many big banks have lost important information about their customers because of huge security failures. The botnet's fast spread and attack on many systems shows how big a threat it is to online safety.

3. **Target Devices**

   X-Bot mostly goes after Windows computers, using flaws in older versions (like Windows 7 and before). Evidence shows that viruses are adapting to infect Internet of Things devices, especially in homes with low security systems [3]. But it does not work well on mobile phones because of strong safety measures in today’s smartphone systems.

4. **Botnet Architecture**

   X-Bot uses a mix design that includes both the P2P and classic client-server setups. It has many scattered command and control servers that make it hard to shut down. Top levels control the bottom ones, making sure multiple paths are available and communication doesn't stop easily.

5. **Botnet Behaviour**

   The main actions of X-Bot are spying on keys, stealing data and starting DDoS attacks. It changes settings in the computer system registry to make it last, hides its network traffic as good and often talks with C &amp, C servers for updates or orders [4]. It can also get extra cargo, change its job according to the target.

6. **Botnet Resilience**

   X-Bot uses special algorithms and techniques to make communication for command centers more resilient. Its code has many backup options to reconnect with control servers. The latter makes it work even if some parts are not secure anymore [4]. Moreover, it hides its presence like a rootkit which makes finding and getting rid of hard.

7. **Botnet Takedown**

   People from international law and cyber security worked together to break down X-Bot.

8. **Botnet Evolution**

   X-Bot has changed a lot since it first developed or discovered. First, a simple software to track keystrokes was created. It then became more advanced and gained skills like stealing computer power for crypto mining and demanding ransomware payments [4]. Moreover, new types of viruses have better ways to hide, showing that those who make them are always improving and changing.

Recommendations

1. **Regular Software Updates and Patch Management:** Often update all kinds of software, mainly operating systems and antivirus programs. This helps shut down security holes that bad bots like X-Bot often use for their own goal. Often, regular updates come with important fixes for newly discovered weaknesses [5]. This significantly reduces the possibility of harmful programs exploiting them.

2. **Advanced Antivirus and Anti-Malware Solutions:** It is very important to use good antivirus and anti-malware programs. These tools are made to find and stop tricky computer viruses, even ones that can get past old ways of finding them.

3. **Robust Firewall Configuration:** Making and tightly controlling all firewall rules is important to keep yourself safe. Firewalls should stop unwanted in or out network traffic while also closely watching for odd things like atypical data packets and big amounts of internet activity. This could signal a botnet is active.

4. **Intrusion Detection and Prevention Systems (IDPS):** Putting IDPS in place is important to protect networks all the time [6]. These systems can find signs of sneaking or dengerous activities that talk about botnet contamination, helping companies make fast and strong responses before big harm happens.

5. **Employee Training and Awareness Programs:** Regular and full cybersecurity training for all workers is very important in a big protection plan. It makes people understand about phishing emails, shows how vital strong password habits are, and teaches them to avoid downloading or installing things from unknown sources.

6. **Regular Data Backups:** Making sure you keep safe copies of all important data and settings regularly is required. If a botnet attack happens, having access to recent backups helps limit information loss and speeds up the healing process.

Conclusion

The investigation into the X-Bot botnet showed it's smart and always changing. This shows how much harm it could do to many types of systems. Important points include its many different looks, a mix design for command and control, plus various ways it can attack like taking data or bombarding websites. But, the research had problems getting real-time data from botnets and copying complex behavior of bots in a safe space. These rules a bit stopped fully understanding the latest versions and complex tricks to avoid detection. This study shows how important it is to always improve cybersecurity. If we get more time, next moves would be to look at real-time data more closely.

References

[1]. S. F. Shetu, M. Saifuzzaman, N. N. Moon, and F. N. Nur, "A survey of botnet in cyber security," in Proc. 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Sep. 2019, pp. 174-177.

[2] W. Li, J. Jin, and J. H. Lee, "Analysis of botnet domain names for IoT cybersecurity," IEEE Access, vol. 7, pp. 94658-94665, 2019.

[3] T. Lange and H. Kettani, "On security threats of botnets to cyber systems," in Proc. 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Mar. 2019, pp. 176-183.

[4] B. Padmavathi and B. Muthukumar, "A deep recursively learning LSTM model to improve cyber security Botnet attack intrusion detection," International Journal of Modeling, Simulation, and Scientific Computing, vol. 14, no. 02, Art. no. 2341018, 2023.

[5] Z. Bederna and T. Szadeczky, "Cyber espionage through Botnets," Security Journal, vol. 33, no. 1, pp. 43-62, 2020.

[6] S. Yamaguchi, "Botnet defense system: Concept, design, and basic strategy," Information, vol. 11, no. 11, Art. no. 516, 2020.