IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311114|

Strengthening Cyber Defense: The Role of Counterintelligence and Counterattack in Threat Intelligence

Shobha Agasibagil, Anusha D S, Bhavya Reddy R

Assistant Professor, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, CIT, Gubbi, Tumkur, Karnataka, India

ABSTRACT: Cyber-attacks on financial and corporate sectors are rising, becoming more advanced and harder to trace due to tools like VPNs that mask attackers' identities. Traditional Cyber Threat Intelligence (CTI) focuses on defense but lacks mechanisms to unmask attackers. This research integrates counterintelligence and counterattack techniques to enhance CTI, bypass VPNs, and exploit adversaries' vulnerabilities. By eliminating persistence mechanisms and tracing attackers' origins, this approach enables early detection, actionable insights, and strengthened defenses, helping organizations identify attack motives and mitigate future threats effectively.

KEYWORDS: Cyber manipulation, adversarial intelligence, active defense, persistence mechanisms, MAC address, network address, virtual private network, remote desktop protocol, secure shell, decoy systems.

I. INTRODUCTION

Cyber-attacks are increasing as attackers exploit weaknesses in people, processes, and technology. Cybercriminals have advanced their tactics to evade detection, with ransomware and other threats affecting many organizations worldwide. While Cyber Threat Intelligence (CTI) has grown to address these issues, it often focuses on defensive strategies, which are insufficient to fully uncover attackers' identities, especially when VPNs and other anonymity tools are used.

This research proposes a comprehensive approach, combining deception, counterintelligence, and counterattack methods to strengthen CTI. Through techniques such as honeytokens, document-based traps, and multi-stage algorithms, we aim to trace attackers back to their origin, even bypassing VPNs to reveal true identities. By enhancing traditional CTI with these proactive strategies, this work seeks to both defend systems and provide critical intelligence on attackers, allowing organizations to respond more effectively and prevent future incidents.

II. RELATED WORK

The authors propose a defensive approach for gathering threat data and monitoring electronic threats, including creating an interactive honeypot using a PDF exploit to identify attackers through reverse TCP. They argue that current cyber threat intelligence (CTI) methods are unreliable and need improvement, suggesting that the field could benefit from intelligence studies methods. Additionally, they highlight a campaign by the Russian-affiliated APT28, using Microsoft OneDrive for command-and-control (C2) operations. This campaign exploits a vulnerability in MSHTML, allowing attackers to sync and execute encrypted commands via OneDrive, which is noted as an innovative technique.

III. METHODOLOGY

This study addresses the underuse of counter-threat intelligence by creating a system that not only prevents cyberattacks but also tracks attackers, even when they use VPNs. The proposed model involves setting up an ESXI server in a data center with both public and private paths to collect attacker logs. It uses honeypots like Cowrie and Windows with open ports (e.g., SSH) to deceiveattackers, while logs are stored and manipulatedto mislead them.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311114|

1.Problem Overview:

- Traditional counter-threat intelligence methods are underused, and the increasing number of cyberattacks requires novel approaches.
- Previous techniques fail when attackers use VPNs, as the basic information, such as IP addresses, becomes masked.
- The study addresses these issues by creating a counterintelligence and counterattack environment, providing tools for tracking and countering attackers.

2. Proposed Environment:

- ESXI Server Setup:The environment is built using an ESXI server in a data center, with public and private paths to capture attacker logs.
- Honeypots such as Cowrie and Windows are used, with open ports like SSH for deception.
- Log Server:Logs are collected securely and accessed via a private path, aiding in the analysis of attacker behavior.
- Deception Mechanism: The system deploys decoy services and machines only visible to attackers, even if they use a VPN or proxy.

3. Proposed Model Architecture:

- System Setup:Uses VMware hypervisor and SDN to support virtual machines running honeypots (low-interaction or high-interaction).
- Ubuntu's Open Virtual Switch (OVS) helps deploy fake Docker containers that respond differently to attackers.
- Interaction and Restrictions:Specific honeypots are deployed to attract attackers based on the country or behavior. Honeypots like Cowrie, Conpot, and Snare Tanner are used for attracting attackers.

4. Counterintelligence Components:

- Honey Token Generation: Undetected by antivirus software, honey tokens conceal Marco's identity while generating harmful tokens.
- Information Gathering:Documents with embedded scripts gather system information about the attacker, such as operating system, network type, and Wi-Fi/ethernet details.
- Geographic Location:The attacker's location is identified using their IP and BSSID to pinpoint geographic location on a map.
- Windows and Linux Tokens:Special tokens are created for Windows (Office documents) and Linux (Libre Office/Open Office) to lure attackers.

5. Malicious Documents:

- Harmful Payloads:Documents are generated with hidden macros to trigger a payload when accessed, providing reverse shell access to the attacker's system.
- Dropper Files:Fake job offers and stolen personal data are used to target victims, activating a backdoor when malicious code is executed.
- Javascript File Dropper:Malicious JavaScript files are embedded in various document formats, which execute malicious payloads when accessed.
- Manual Attacks Using Shell:Once tokens are obtained, attackers are granted reverse shell access, allowing further operations within their system.

6. Counterattack Management:

- Response to Attacker: Once the attacker accesses the honeypot, counterattack mechanisms are triggered, enabling countermeasures to neutralize the threat.
- Shell Access for Attack Continuation:The system provides shell access for further attacks, keeping the connection open through a backdoor to execute additional commands.

7. Data Analysis and Payloads:

- Multistage Algorithm:Excel is used to run multi-stage processes for bypassing VPNs and creating malicious documents. The algorithm helps beat VPN masking techniques.
- Payloads:Different file types, such as VBA scripts, PE files, OLE files, and PS1 scripts, are used in the counterintelligence and counterattack strategy.
- Payloads are triggered when attackers open documents or run macros, notifying users of malicious actions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311114|

8. Evaluation:

This research offers an innovative approach by using deception, dynamic tokens, and reverse shell techniques to gain insights into attacker systems and thwart ongoing cyberattacks.

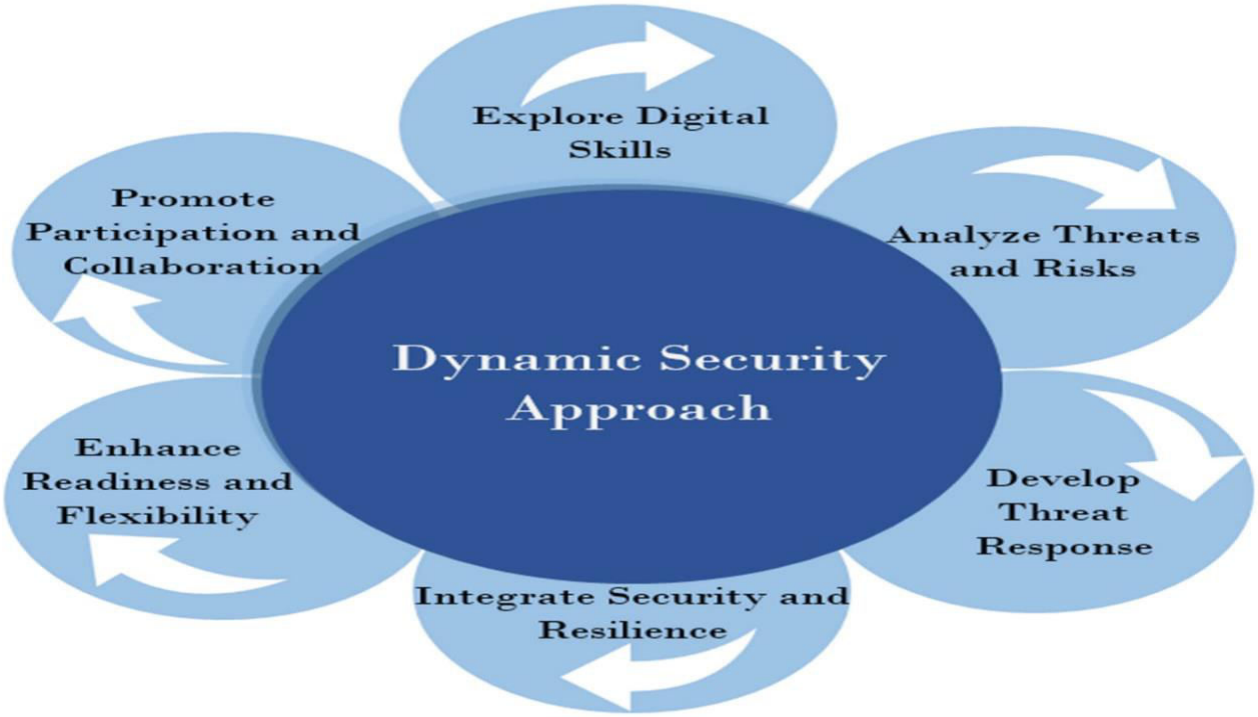

FIGURE 1 : PROPOSED METHODOLOGY DIAGRAM

IV.EXPERIMENTAL RESULTS

The experimental setup aimed to validate the effectiveness of the proposed counterintelligence and counterattack strategy by simulating various cyberattack scenarios. The key findings from the evaluation include:

1. Effectiveness of Honeypots and Deception Mechanisms:

- The deployed honeypots, including Cowrie, Conpot, and Snare Tanner, successfully attracted attackers, even when VPNs and proxies were in use. This indicates the system's ability to deceive attackers and gather critical data despite masking techniques.
- The decoy services were effective in keeping attackers engaged, allowing the system to gather information on their methods and systems.

2. Honey Token Success:

- Honey tokens were successful in gathering system information from attackers. The embedded scripts provided accurate details on attacker behaviour, such as operating system type, network configuration, and other identifying factors.
- Tokens designed for both Windows and Linux platforms proved useful in capturing valuable attack data.

3. Malicious Document Payload Execution:

- The hidden payloads within malicious documents (including macro-triggered reverse shell access and dropper files) executed as intended. Once attackers opened the documents, they triggered the payloads, providing shell access to their systems.
- The malicious JavaScript file droppers embedded in documents successfully executed when accessed, delivering reverse shells and enabling further operations.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311114|

4. Counterattack Mechanisms:

- Once attackers interacted with the honeypots and tokens, the system's counterattack mechanisms were triggered. These countermeasures included the deployment of reverse shell access and dynamic payload execution, which allowed the system to neutralize the attackers and limit further actions.
- Shell access granted attackers the ability to continue operations, but the system monitored and responded with countermeasures that halted or contained the attack.

5. Bypassing VPN and Proxy Techniques:

- The multistage algorithm, integrated with Excel for bypassing VPN masking techniques, was highly effective in identifying the real location of attackers and circumventing VPNs. This allowed for a more accurate geographic location mapping and an enhanced understanding of the attacker's infrastructure.
- Various payloads (VBA scripts, PE files, OLE files, PS1 scripts) were tested for their ability to penetrate masked connections, and the results indicated successful payload delivery despite the use of VPNs.

6. Data Collection and Analysis:

- Data collected from the honeypots and malicious documents enabled detailed analysis of attacker behaviour and system identification. The system's ability to track and store attacker actions provided valuable insights into threat patterns, which can be used for improving future defences.

7. Overall System Performance:

- The combination of dynamic deception, token generation, and reverse shell access made the counterintelligence system effective at thwarting cyberattacks while also gathering intelligence on attacker tactics, techniques, and procedures (TTPs).
- The setup was stable and efficient in both capturing attacker data and implementing countermeasures in real time, showcasing its potential as a viable counterintelligence tool.

In conclusion, the experimental results demonstrate that the proposed counterintelligence and counterattack strategy is effective in countering cyber threats, particularly in overcoming VPN masking, gathering valuable attacker data, and deploying countermeasures to neutralize attacks.

V.CONCLUSION

Defending against cyberattacks is challenging as attackers constantly evolve their methods. Traditional detection struggles with evasion techniques like VPNs, which maintain persistence even after a system reboot. To counter this, we remove malicious programs from the registry and start menu. Our proposed method uses a "Counterattack" function to gather real IP addresses, system info, and running processes, and a "Counterintelligence" function to extract attacker data through malicious documents (e.g., Word, PowerPoint, Excel). This approach focuses on revealing the attacker's identity and improving threat recognition, unlike traditional methods that only address known threats.

Defending against cyberattacks is increasingly challenging for organizations, as attackers continuously refine their methods to infiltrate networks. Identifying a breach after it has occurred is a difficult task due to the constant evolution of evasion tactics. Even after a security breach, attackers can access sensitive information. Many hackers leverage paid VPN services to ensure their persistence within a network, with these VPNs automatically reconnecting after a reboot, allowing the attacker to maintain access. To combat this, our approach involves removing such programs from both the system registry and the start menu.

REFERENCES

[1]. Rana, M. U., Ellahi, O., Alam, M., Webber, J. L., Mehbodniya, A., Khan, S. (2022). "OffensiveSecurity:Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack." IEEE Access.
[2]. Bayraktar, G. (2014). "The new Requirement for a Fifth Dimension of War: Cyber Intelligence." ICCWS 2014.
[3]. Azzini, L., & Schneider, R. (2021). "Enhancing Offensive Cybersecurity Strategies with Real-Time Counterintelligence." IEEE Security & Privacy.
[4]. Schmitt, M. N. (2013). "The Regulation of Cyber Warfare." International Law Studies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311114|

[5]. Möller, T., et al. (2018). “Cyber Counterintelligence: Exploring Offensive Tools for Intelligence Gathering.” Journal of Information Warfare.
[6]. Ackerman, M. S. (2020). “Cyber Countermeasures and Offensive Security.” Journal of Strategic Cybersecurity.
[7]. Mellado, D., et al. (2012). “Cybersecurity Risk Management in Offensive Security and Counterintelligence.” Springer.
[8]. Rana, M. U., & Khan, S. (2021). “Developing Counterattack Mechanisms for Cyber Resilience.” International Journal of Computer Science.
[9]. Khan, S., et al. (2023). “Advanced Counterintelligence Techniques for Cyber Operations.” IEEE Transactions on Cybersecurity.
[10]. Zetter, K. (2014). “Hacking Back: Legal and Ethical Dimensions of Cyber Counterattacks.” International Journal of Law and Cyber Warfare.
[11]. K. Oosthoek and C. Doerr, "Cyber threat intelligence: A product without a process?" Int. J. Intell. Counterintell., vol. 34, no. 2, pp. 300–315, Jul. 2020, doi: 10.1080/08850607.2020.1780062.
[12].P. Karuna, H. Purohit, S. Jajodia, R. Ganesan, and O. Uzuner, "Fake document generation for cyber deception by manipulating text comprehensibility," IEEE Syst. J., vol. 15, no. 1, pp. 835–845, Mar. 2021, doi: 10.1109/JSYST.2020.2980177.
[13].N. C. Abay, C. G. Akcora, Y. Zhou, M. Kantarcioglu, and B. Thuraisingham, "Using deep learning to generate relational HoneyData," in Autonomous Cyber Deception, 2019, pp. 3–19, doi: 10.1007/978-3-030-02110-8_1.
[14].S. Fugate and K. Ferguson-Walter, "Artificial intelligence and game theory models for defending critical networks with cyber deception," AI Mag., vol. 40, no. 1, pp. 49–62, Mar. 2019, doi: 10.1609/aimag.v40i1.2849.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details