ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

UDC 004.056

COMBATTING QAKBOT: A REVIEW OF DETECTION AND ANALYSIS TECHNIQUES

Aisulu Zhangeldi Zhanibekkyzy
aisulu26012002@gmail.com
Master's student at the Faculty of Information Technologies of L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Scientific supervisor – S. Santeyeva

Qakbot, a multi-faceted botnet, continues to pose a significant threat to organizations worldwide. Its ability to steal sensitive data, deploy ransomware, and disrupt critical operations necessitates robust detection and analysis methods. This paper reviews the current state of the art in Qakbot analysis, examining existing techniques, their limitations, and promising avenues for future research. We discuss traditional signature-based and endpoint detection and response (EDR) approaches, highlighting their vulnerabilities to evasion techniques. We then explore network traffic analysis (NTA) and machine learning as emerging solutions, emphasizing their potential and challenges. Finally, we propose promising research directions, including deep learning, behavioral analysis, and cross-layer analysis, to strengthen Qakbot detection and analysis capabilities. This review aims to inform and guide researchers and practitioners in developing effective strategies to combat this evolving threat.

Keywords: Qakbot, Malware Analysis, Network Traffic Analysis, Machine Learning, Cybersecurity

QakBot, also referred to as Qbot, Quackbot, Pinkslipbot, and TA570, has been a prolific force in the global malware landscape, responsible for numerous infections worldwide, particularly within the Financial Sector. Originating around 2008, QakBot initially functioned as a banking trojan, primarily utilized to pilfer banking credentials through phishing campaigns featuring malicious attachments or download links. Over time, it has undergone significant evolution, transforming into a versatile botnet and malware variant with diverse capabilities[1].

Previously, Qakbot's campaigns were mostly distributed through “pray-and-spray” spam campaigns. However, Qakbot's modular design played a major role in its success in attracting dinero, or bitcoin, as it may be called, through the following optional modules [2]:

- Email Collection Module: All emails are extracted from the local Outlook client using this well liked add-on, and the email addresses are subsequently used to launch fresh phishing attacks. By replying to an infected host's previous email threads with a malicious attachment or link, a secondary email function allows additional infections by causing the new victim to inadvertently download Qakbot malware.
- The Universal Plug-and-Play (UPuP) module has the ability to turn compromised systems without direct Internet access into middle command-and-control (C2) servers that the botnet may employ.
- Cookie Grabber Module: This module takes cookies from widely used browsers, just what it says on the box.
- Web-Inject Module: Qakbot supplies JavaScript code to the malware injector module along with a specified list of dangerous and/or "poisoned" websites (many of which were disseminated by Qakbot's spam campaigns). Should the targeted victim visit any of these websites, JavaScript code will be injected. Usually, this module was used to financial firms.

This adaptability, coupled with its ability to evade traditional detection methods, makes Qakbot a formidable opponent. Signature-based approaches often fall short against the botnet's ever-changing code, as research by Javier Vicente (2024) highlights, noting its modular architecture and frequent

updates render such methods ineffective. Similarly, endpoint detection and response tools may struggle to keep pace with Qakbot's sophisticated evasion techniques, including process injection, anti-debugging, and sandbox detection bypasses. This highlights the clear need for robust and innovative Qakbot analysis methods, as the limitations of traditional approaches are increasingly evident.

This review aims to shed light on this evolving threat, delving into the existing techniques used to detect and analyze Qakbot activity. We will examine their strengths and limitations, highlighting the challenges that hinder effective mitigation. Moreover, we will explore promising avenues for future research, showcasing cutting-edge approaches that hold the potential to outmaneuver this persistent adversary. By providing a comprehensive understanding of Qakbot and its vulnerabilities, we hope to empower researchers and practitioners to develop the next generation of defenses against this ever-evolving threat.

Understanding the qakbot threat. Qakbot primarily infiltrates systems through phishing emails disguised as legitimate communications, often containing malicious attachments or links that install the malware upon opening. Once installed, it establishes communication with its command-and-control (C2) server, enabling attackers to remotely control the infected system and execute malicious activities [2]. Qakbot's capabilities extend beyond basic data theft, encompassing:

- Ransomware Deployment: Qakbot can deploy various ransomware strains, encrypting critical data and demanding ransom payments for its decryption, leading to significant financial losses and operational disruption.
- Lateral Movement: Qakbot can spread laterally within networks, infecting additional systems and expanding its reach, making containment efforts more challenging [3, 4].
- Data Exfiltration: Qakbot can steal a wide range of sensitive data, including login credentials, credit card information, and financial records [4]. This stolen data can be used for financial gain by the attackers, or potentially sold on the dark web where stolen information is a valuable commodity for criminal activities [5].

Existing Qakbot Analysis Techniques:

Traditional approaches to Qakbot detection and analysis face limitations:

- Signature-Based Techniques: While signature-based detection offers speed, efficiency, and accuracy against known phishing attempts, its reliance on pre-defined signatures and limited scope render it vulnerable to evolving tactics and sophisticated attacks, necessitating regular updates and exploration of broader detection methods [6].
- Endpoint Detection and Response (EDR): Endpoint Detection and Response (EDR) solutions offer significant advantages, including rapid analysis, proactive threat identification, and automated responses. They also improve Mean Time to Respond (MTTR) and overall security posture. However, EDR tools have limitations, such as limited scope, complexity, and reliance on additional resources, requiring careful consideration alongside their benefits when building an organization's cybersecurity strategy [7].

Emerging solutions offer promising alternatives:

- Network Traffic Analysis (NTA): While network analysis offers a powerful approach to identify and classify IoT devices using machine learning, its application for specifically detecting malware like Qakbot requires a different perspective. Unlike typical IoT devices with unique network fingerprints, Qakbot's strength lies in its ability to evade detection through techniques like code obfuscation and dynamic loading. Network analysis for Qakbot detection should focus on identifying anomalous traffic patterns rather than device fingerprinting. This could involve searching for unusual data exfiltration attempts, communication with suspicious IP addresses or domains potentially associated with Qakbot's C2 infrastructure, or specific network protocols known to be used by this malware [8]. By tailoring network analysis techniques to Qakbot's behavior, security professionals can enhance their ability to detect and mitigate this evolving threat.
- Machine Learning: Incorporating machine learning into Qakbot malware analysis processes presents significant advantages, including enhanced detection accuracy by identifying patterns and anomalies more effectively, scalability to handle the evolving tactics of Qakbot variants, faster analysis enabling rapid response to emerging threats, and adaptability to counter new iterations

of Qakbot. However, challenges persist, such as the risk of Qakbot developers designing evasion techniques against machine learning models, dependence on high-quality and unbiased data, interpretability issues with complex models, and resource-intensive model training. Addressing these challenges requires a comprehensive approach tailored to Qakbot's unique characteristics, aiming to maximize the benefits of machine learning while mitigating associated risks in effectively combating Qakbot infections [9].

Limitations and Promising Avenues for Future Research:

Several limitations hinder the effectiveness of existing Qakbot analysis methods:

- Evasion Techniques: Qakbot's adaptability and evasion techniques, such as code obfuscation and dynamic loading, can bypass traditional detection mechanisms.
- Limited Visibility: Endpoint-based approaches may lack visibility into encrypted traffic or traffic originating from compromised external devices.
- False Positives: NTA and machine learning methods can generate false-positive detections, leading to wasted resources and analysis overhead.
- Data Availability: Access to real-world Qakbot-infected network traffic data can be limited, hindering the development and evaluation of effective detection and analysis methods.

Promising research avenues exist to address these limitations:

- Deep Learning: Deep learning algorithms like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) hold promise for analyzing complex network traffic patterns and identifying Qakbot activity with high accuracy.
- Behavioral Analysis: Analyzing Qakbot's behavior within infected systems can provide valuable insights into its capabilities and intentions, leading to more robust detection and analysis methods.
- Threat Intelligence Integration: Integrating threat intelligence feeds with NTA and machine learning models can improve the detection of emerging Qakbot variants and enhance overall analysis effectiveness.
- Cross-Layer Analysis: Combining network traffic analysis with endpoint data and file analysis can provide a holistic view of Qakbot activity. This approach allows for correlating network traffic anomalies with events observed within the system, strengthening detection accuracy and facilitating comprehensive analysis of Qakbot's actions.
- Real-Time Analysis: Developing real-time Qakbot analysis methods is crucial for prompt detection and response to attacks. This can be achieved through continuous monitoring of network traffic and employing algorithms capable of identifying anomalies in real-time, minimizing potential damage and disruption caused by Qakbot activity.

Conclusion

Qakbot remains a significant threat due to its constant evolution and evasion techniques. Existing detection and analysis methods face limitations, including vulnerability to evasion, limited visibility, and false positives. Promising avenues for future research lie in deep learning, behavioral analysis, threat intelligence integration, cross-layer analysis, and real-time analysis. By exploring these avenues, researchers and practitioners can develop more robust and effective Qakbot analysis capabilities, ultimately strengthening cybersecurity posture and protecting organizations from this evolving adversary.

References

1. CISA. (2023, August 30). Identification and Disruption of QakBot Infrastructure. https://www.cisa.gov/sites/default/files/2023-08/AA23-242A.stix_.xml

2. Blackberry. (2023, October 26). Inside the FBI and DoJ Takedown of Qakbot, the Swiss Army Knife of Malware. https://blogs.blackberry.com/en/home

3. MITRE ATT&CK. (n.d.). QakBot. Retrieved March 8, 2024, from https://attack.mitre.org/software/S0650/

4. Bleeping Computer. (2023, September 22). QBot Needs Only 30 Minutes to Steal Your Credentials and Emails. https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-

minutes-to-steal-your-credentials-emails/
5. Dark Reading. (2023, October 26). Sale of Stolen Credentials and Initial Access Dominate Dark Web Markets. https://www.darkreading.com/threat-intelligence/sale-of-stolen-credentials-and-initial-access-dominate-dark-web-markets
6. Insights2TechInfo. (2023, November 10). Unveiling the Strengths and Limitations of Signature-Based Phishing Detection. https://par.nsf.gov/servlets/purl/10346590
7. Roy, R. (2019). Network Traffic Analysis based IoT Device Identification. 2019 IEEE International Conference on Computational Intelligence and Intelligent Systems (CIS).
8. Roy, S., Aich, S., Goswami, A., & Mukhopadhyay, S. (2020, September). Adversarial Attacks on Deep Learning Models in Text Classification. **https://arxiv.org/abs/2009.04682**
9. Zhao, D., Wang, Y., & Li, J. (2018). An Efficient Content-Based Image Retrieval Method Using Local Feature Matching and Multi-Scale Block Matching. ScienceDirect, 133, 130-142. https://www.sciencedirect.com/science/article/pii/S1047320320302145

UDC 004.056.53

EXPLORING THE POTENTIAL OF SYSMON TO DETECT AND ANALYZE ATTACKS IN REAL TIME

Bakhytov Bigasyr Armanovich
bigasyr@gmail.com
Научный руководитель – Н. Ташатов
Кандидат физико-математических наук, доктор Ph.D, доцент
tash.nur@mail.ru

Abstract. The ever-evolving landscape of cybersecurity threats necessitates constant innovation in detection and analysis techniques to safeguard digital assets. In this context, Sysmon emerges as a promising tool for real-time monitoring and analysis of system activity on Windows-based environments. This research paper aims to explore the potential of Sysmon in detecting and analyzing attacks as they occur in real time. By leveraging Sysmon's rich set of event logs and advanced filtering capabilities, security analysts can gain deeper insights into system-level activities, identify anomalous behavior indicative of cyber threats, and respond promptly to mitigate risks. This paper elucidates the efficacy of Sysmon in enhancing the resilience of organizations against a diverse range of cyber-attacks, including malware infections, unauthorized access attempts, and data exfiltration.

Keywords. Sysmon, Sysinternals, Network connection, SwiftOnSecurity Sysmon Config, OlafHartong Sysmon Config, Advanced Threat Detection, real-time attack detection

1. Introduction

Sysmon, developed by Microsoft and made freely available as part of the Sysinternals suite, offers comprehensive visibility into system-level activities through the generation of detailed event logs. Unlike traditional logging mechanisms, Sysmon provides granular insights into processes, network connections, file modifications, registry changes, and other critical system events.

By leveraging Sysmon's capabilities, organizations can enhance their ability to detect a wide range of cyber threats, including malware infections, insider threats, and advanced persistent threats (APTs).

Configuring Sysmon to balance detection accuracy with performance overhead requires careful consideration of various factors, including event filtering, data aggregation, and resource utilization. Additionally, interpreting Sysmon logs and distinguishing security incidents from benign activities demand specialized knowledge and expertise.

2. Installing and configuring the Sysmon.

Download Sysmon from the official Microsoft website – https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon.

Install with default options (hashed images with SHA1 and no network monitoring):