Combatting the TrickBot Threat: Analysis, Impact, and Defensive Strategies in Cybersecurity

Jintao Cao*, Allie Null*, Marissa Stewart*, Suman Bhunia*, Mohammed Salman†
*Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA
†College of Computer, University of Anbar, Anbar, Iraq
Email: {caoj22, nullak, stewa102, bhunias}@miamioh.edu, mohammed_salman@uoanbar.edu.iq

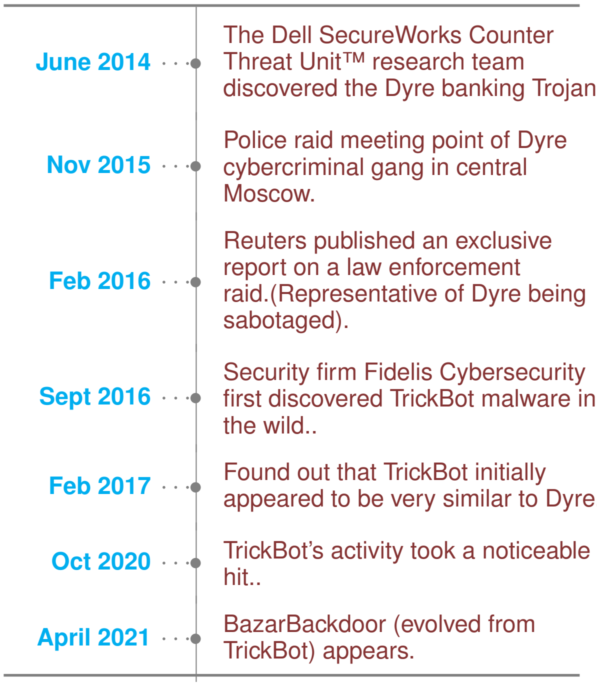
***Abstract*—The TrickBot Botnet, emerging in late 2016, has been a significant cybersecurity threat, leveraging sophisticated attack vectors such as phishing emails, network vulnerabilities, and secondary payloads. This paper provides a comprehensive analysis of TrickBot's evolution, attack methodologies, and widespread impact on individual users, businesses, and government entities. Despite some disruptions to its infrastructure, TrickBot has demonstrated remarkable resilience, continually adapting its tactics to evade detection and enhance its malicious capabilities. Our research offers detailed insights into the operational mechanisms of TrickBot, supported by extensive data on its propagation and impact. Furthermore, we evaluate various defense strategies, including advanced technical measures and human-centric approaches, to mitigate the ongoing threat posed by TrickBot and similar botnets. The findings underscore the critical need for continuous vigilance and innovation in cybersecurity practices to effectively counter such persistent threats.**

***Index Terms*—TrickBot Botnet, Malware, Ransomware, Security, Banking Trojan, Cyber-attacks**

I. Introduction

In November 2015, Russian law enforcement authorities conducted a raid on a high-rise building in central Moscow, effectively disrupting the operations of a cybercrime syndicate responsible for the Dyre Bank Trojan. This event was subsequently reported in a Forbes article, which provided insights suggesting the high-level apprehension of members associated with the Dyre group. The significance of Dyre in the realm of cybersecurity has been profound since its initial identification by the Dell SecureWorks Counter Threat Unit™ (CTU™) research team in early June 2014. The successful intervention by the authorities was met with widespread approval. Nonetheless, in retrospect, this triumph appears to have been a mere precursor to a more extensive cybersecurity crisis [1].

In September 2016, a year following the aforementioned raid, Fidelis Cybersecurity initially detected a new malware on their systems. Subsequently named the TrickBot Botnet, this banking Trojan emerged as a formidable cybersecurity threat over the ensuing five years. Initially, TrickBot did not garner significant attention, mirroring the early stages of other minor Trojans. Its initial versions, while technically competent, were narrowly focused on select regional banks in the United States [2]. Characteristic of banking Trojans, TrickBot maintains a list of targeted websites, manipulating web traffic to capture sensitive information and redirect financial transactions. Despite its inherent programming limitations, TrickBot's capacity for propagation was initially underestimated. The malware's rapid development posed significant challenges for cybersecurity experts, adapting continuously to target an evolving roster of online banking platforms. During this period, TrickBot garnered considerable attention from the cybersecurity community. Analysis revealed that its initial component, dubbed TrickLoader, bore striking similarities to the Dyre Trojan. Notably, TrickBot surpassed Dyre in aspects of penetration, propagation, and stealth. In response, cybersecurity professionals across various sectors mobilized defenses against TrickBot. Nevertheless, the malware proved to be an elusive and multifaceted threat, adept at compromising banking systems and websites with minimal detectable presence.



June 2014	The Dell SecureWorks Counter Threat Unit™ research team discovered the Dyre banking Trojan.
Nov 2015	Police raid meeting point of Dyre cybercriminal gang in central Moscow.
Feb 2016	Reuters published an exclusive report on a law enforcement raid.(Representative of Dyre being sabotaged).
Sept 2016	Security firm Fidelis Cybersecurity first discovered TrickBot malware in the wild..
Feb 2017	Found out that TrickBot initially appeared to be very similar to Dyre.
Oct 2020	TrickBot's activity took a noticeable hit..
April 2021	BazarBackdoor (evolved from TrickBot) appears.

Figure 1: Timeline of TrickBot.

Our research indicates that the confrontation between cybersecurity experts and the TrickBot Botnet malware has been relentless, characterized by a continuous escalation with no discernible drawbacks. Cybersecurity professionals have devised a variety of strategies to neutralize and eradicate the TrickBot Botnet at its source, during transmission, and at the endpoint. These strategies include proactive measures targeting the devices of the attackers themselves. Each time the TrickBot malware is neutralized, it re-emerges to challenge the security systems with enhanced capabilities. This ongoing conflict persisted until early 2021. A significant setback for TrickBot occurred in October 2020, when a concerted effort by U.S. Cyber Command and a coalition of private security firms, spearheaded by Microsoft, succeeded in disrupting much of its infrastructure. This intervention compelled the malware's developers to escalate and refine their tactics. In a similar vein to Dyre, TrickBot resurfaced in mid-2021, introducing new Trojans such as Emotet and BazarBackdoor, which continue to pose a significant threat to global cybersecurity [3]. Figure 1 delineates the general timeline of the discovery and activities of the TrickBot Botnet.

This article aims to provide a comprehensive and professional analysis of the TrickBot malware. The main contributions of this paper are:

- A comprehensive analysis of the TrickBot Botnet, including its evolution, attack methodologies, and the various stages of its development.
- Detailed insights into the impact of TrickBot across different sectors, highlighting its global reach and the variety of targets, ranging from individual users to large corporations and government entities.
- A review of defense solutions against TrickBot, encompassing both general strategies for combating botnets and specific tactics for countering TrickBot, including technological measures and human-centric approaches like training and awareness.

The rest of the paper is organized as follows. Section II is dedicated to establishing the foundational context of the TrickBot malware, addressing fundamental questions such as its nature and origins. In Section III, we leverage our expertise to elucidate the mechanisms of TrickBot's attack strategies, examining the reasons behind its potency and the challenges inherent in mitigating its impact. Section IV presents an in-depth analysis, supported by extensive data, to assess the detrimental effects of the TrickBot malware on nations, corporations, and individuals over its five-year prevalence. Finally, Section V synthesizes research from various cybersecurity domains to dissect how TrickBot has been compromised, from the user's endpoint to its source, and to outline effective defense strategies against potential TrickBot-related cyber threats.

II. Background

The concept of a "botnet" is derived from the amalgamation of the terms "robot" and "network." Botnets constitute networks of compromised computer systems utilized for executing cyber-attacks [4]. They facilitate automated mass-scale offensive operations, encompassing activities such as data theft, server disruption, and malware propagation. One of the notable functions of botnets is their ability to disseminate spam messages in extraordinarily large volumes, leveraging automation for efficiency. For instance, the Cutwail Botnet, utilizing such automation, is capable of dispatching up to 74 billion messages per day, a rate unattainable by human efforts. Additionally, botnets possess the capability to proliferate malware, thereby expanding their network through the infection of additional computer systems.

The construction of a botnet encompasses three distinct stages: 1) Preparation and Exposure, 2) Infection, and 3) Activation. During the Preparation and Exposure phase, attackers exploit vulnerabilities in the targeted system, thereby exposing users to malware. These vulnerabilities can be identified in websites, applications, and even in human behavior, underscoring that they are not exclusively technological in nature. Subsequently, in the Infection stage, malware infiltrates users' devices within the system, granting the botnet unfettered control over the compromised devices. Infection methods range from deceiving users into downloading a Trojan virus to automatic malware downloads upon visiting an infected website. The final stage, Activation, enables attackers to orchestrate operations using all infected devices within the system. At this juncture, attackers consolidate the infected devices into a cohesive network of bots—forming the "botnet"—which can be remotely controlled. The significant risk posed by this malware stems from its ability to facilitate administrative-level access through the infected devices.

Botnets are predominantly employed for a variety of malicious activities, including financial and information theft, service sabotage, cryptocurrency fraud, and the sale of access to these networks to other criminals. The primary motivation behind the creation and deployment of botnets is typically the financial or personal benefit of the perpetrator. While botnets themselves represent a formidable cyber threat, they also serve as facilitators for secondary attacks on already compromised computers. These ancillary attacks encompass tactics such as distributed denial-of-service (DDoS), phishing, and brute-force attacks. Given the prevalent vulnerabilities in many devices, it is imperative for users to exercise heightened vigilance against botnet threats.

The TrickBot Botnet, emerging in October 2016, is a banking Trojan known by various aliases, such as The Trick and TrickLoader. By 2017, TrickBot had extended its operations globally, targeting prominent banks across multiple countries, including but not limited to the United Kingdom, the United States, Switzerland, Germany, Canada, New Zealand, France, and Ireland [5].

TrickBot is posited to have originated from an antecedent botnet, known as Dyre or Dyreza, through a process of code restructuring and optimization. The criminal entity orchestrating TrickBot perpetually refines its malware, incorporating new modules with additional functionalities and frequently altering IP addresses and host systems. These continual updates not only augment the malware's efficacy and potential for damage but also pose significant challenges to network security

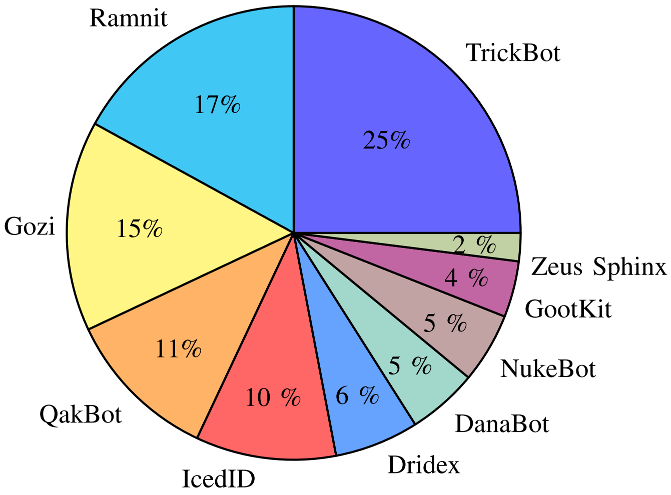


Figure 2: A pie chart showing 2019's most prevalent malware to date, with TrickBot being the most prevalent (source: IBM X-Force)

systems, professionals, and agencies in promptly detecting and thoroughly neutralizing it. While various strategies have been employed to identify and counteract TrickBot, thereby mitigating certain losses, achieving complete immunity against TrickBot attacks remains a formidable challenge. Most countermeasures tend to increase operational costs for the criminal groups managing the botnet rather than eliminating the threat posed by TrickBot entirely [6].

Over the past two years, as TrickBot has evolved in capability and sophistication, it has demonstrated an increased resilience against existing defenses against Trojans and ransomware, affecting a broader range of sites. Check Point's research reveals that in the last 16 months, TrickBot has infected over 140,000 machines, implicating clients from 60 corporations. Notable affected entities include Amazon, Microsoft, PayPal, Bank of America, Wells Fargo, and American Express [7]. Concurrently, the strategies for detecting and countering TrickBot have undergone significant evolution. Initially, efforts focused on identifying TrickBot's Command and Control (C2) servers and nullifying the IP addresses they utilized, an approach aimed at disrupting the botnet by transmitting configuration files to infected computers to sever their connection to the C2 infrastructure. With ongoing technological advancements, there is a growing optimism that the complete eradication of TrickBot may be achievable in the future. Figure 2 illustrates the prevalence of the TrickBot Botnet in comparison to other prominent malware strains in 2019.

III. Attack Methodology

TrickBot initiates its attack sequence by specifically targeting Windows-based systems [8] and meticulously monitoring the network traffic of selected banking institutions. Subsequently, it exfiltrates sensitive user account information, primarily usernames and passwords. The dissemination of the TrickBot Botnet malware predominantly occurs through email, designed to deceive victims into activating harmful binary code upon opening compromised messages. A significant risk arises from the users inadvertently accessing emails embedded with scripts that trigger the automatic download of malware onto their devices. The heightened peril of TrickBot stems from its phishing emails, which are adeptly masqueraded as routine communications from the user's bank, thereby rendering detection challenging. The moniker "TrickBot Trojan" is derived from its use of a Trojan horse strategy, presenting seemingly innocuous links that ultimately facilitate the installation of malicious software. The attack methodologies employed encompass a spectrum of tactics such as spear-phishing, exploiting network vulnerabilities, delivering secondary payloads, cookie and remote application playback, and viral deployment. Furthermore, TrickBot's attack strategies are not static; they have evolved to include sophisticated techniques enabling access to system boot processes and the exploitation of backdoors [9].

TrickBot initiates infection when a victim interacts with a malicious link or visits a webpage embedded with malware. Upon successful infiltration, the virus establishes various attack vectors, namely SpearPhishing, Network Vulnerabilities, and Secondary Payloads [5].

SpearPhishing involves the dissemination of malware via infected phishing links, compromised files, malicious URLs, and targeted emails that specifically focus on banks, corporations, and their executives.

Network Vulnerabilities represent another vector, whereby TrickBot leverages the Server Message Block Protocol. This protocol facilitates the spread of the virus across all Windows-operated computers within the targeted organization's network, thereby enabling information propagation among interconnected systems.

Secondary Payload serves as a third vector. In this context, TrickBot is disseminated by Emotet, which is an independent Trojan malware. This approach underscores the complexity and layered nature of TrickBot's distribution mechanisms.

TrickBot employs five principal tactics to compromise networks: Persistence Module, Explicit Routing and Server-Side Injection, Cookie Playback, Remote Application Playback, and Viral Deployment.

The **Persistence Module** allows TrickBot to operate undetected by end-users, concealing its presence through the creation of a scheduled task. This module ensures the malware's continuous operation within the infected system.

Explicit Routing and Server-Side Injection involve the exploitation of existing vulnerabilities, such as explicit redirects and server-side injections. This tactic is employed to capture user information during banking website sessions, granting TrickBot access to victims' financial and personal banking data.

Cookie Playback targets users who do not adequately protect their information. It collects data such as login statuses, website preferences, and personalized content, thereby breaching user privacy.

Remote Application Playback is designed to gather credentials from remote desktop applications, extending TrickBot's impact across various applications within the network.

Finally, **Viral Deployment** leverages infected computers to disseminate spam emails, appearing as if they originate from trusted accounts. Given that TrickBot has access to over 300 million email accounts, this module poses a significant threat due to its capacity to masquerade as legitimate communication.

These diverse and sophisticated methods underscore the complexity and danger of TrickBot in compromising network security.

Upon successful infiltration, TrickBot replicates its payload under a randomly generated name and establishes a scheduled task that executes the copied file with SYSTEM privileges. The core payload of TrickBot is structured as a 32-bit Portable Executable (PE) file. However, it possesses the capability to operate with files compatible with both 32- and 64-bit architectures. The malware conducts a system check to determine the operating architecture and selects the corresponding payload version accordingly. This transition from 32-bit to 64-bit compatibility employs a technique known as Heaven's Gate, a method of misdirection on Windows systems first identified in the mid-2000s [10]. In the context of TrickBot, the shell codes for both 32-bit and 64-bit architectures function similarly, despite their inherent architectural differences. This demonstrates the malware's adaptability and sophistication in circumventing system defenses.

The criminal entity orchestrating TrickBot operations is recognized as a cybercrime syndicate [5]. Presently, two individuals, Alla Witte and Vladimir Dunaev, have been purportedly identified as primary actors within this group. Witte, also known by the alias 'Max,' faces legal charges related to her involvement with the TrickBot group [11]. It is important to note, however, that the operation of TrickBot extended beyond these individuals, with activities spanning multiple countries, including Russia, Belarus, Ukraine, and Suriname [11]. The primary victims of TrickBot were individuals and entities deceived into downloading malicious software via email. The malware specifically targeted major banks worldwide, with a particular focus on institutions and their customers in Northern Ohio. Since its inception in 2015, the group's objective has been to maximize the reach of their attacks.

Over time, TrickBot has undergone significant evolution, transforming into a versatile platform whose capabilities extend well beyond the theft of online banking credentials [12]. In recent developments, TrickBot has been repurposed as a tool for intrusion and reconnaissance, rather than functioning solely as a conventional banking Trojan. Consequently, its creators have begun monetizing access to corporate networks, selling this privileged information to other hackers for the deployment of additional malware. This shift in operation underscores the adaptability and evolving threat landscape posed by TrickBot.

IV. Impact

The TrickBot Botnet, with its exceptional propagation and penetration capabilities, has been a persistent and influential malware since its emergence in 2016. According to Check Point Research, it maintained its position as the most prevalent malware, affecting 4% of organizations globally as of December 2021 [13]. Table 1 presents the top malware families of 2021, along with their usage ratios.

Table I: Table of December 2021's Top Malware Families

Name of the Malware:	Popularity Ranking:	Use Ratio:
Trickbot	1	4%
Emotet	2	3%
Formbook	3	3%
Agent Tesla	4	3%
Glupteba	5	2%
Remcos	6	1%

As of January 2022, TrickBot Botnet still ranks second in prevalence, affecting 4% of organizations worldwide [14]. The resurgence of Emotet in 2022 began with TrickBot, which was observed pushing commands to its bots for downloading and executing Emotet samples on November 14, 2021, marking Emotet's return [15]. Consequently, a significant portion of Emotet's current strength is attributed to TrickBot Botnet's influence.

The diverse and widespread nature of TrickBot Botnet's victims includes individuals, small and medium-sized enterprises, large corporations, and national-level departments and institutions. BitSight researchers found in March 2020 that home office networks were 3.5 times more likely to be infected with malware than corporate networks, with TrickBot malware appearing at least 3.75 times more frequently [16]. By the end of 2021, it had compromised at least 250 million email accounts, including significant numbers from major email providers [17]. TrickBot can install backdoors in compromised systems for remote access, leading to the theft of messages, passwords, user data, and accounts. The compromised computers then become part of the botnet, aiding in the malware's propagation.

Significantly, many email addresses belonging to government workers were also compromised, including those from key U.S. departments [17]. TrickBot Botnet thus presents a considerable threat to national-level departments and agencies. During the 2020 U.S. Presidential Election, it was identified as one of the major threats, with potential to disrupt electoral processes [18]. In September 2020, Trickbot was instrumental in an attack against Universal Health Services, leading to significant operational disruptions [18].

The impact on businesses has been equally severe. TrickBot's method of gaining persistence and exploiting SMB vulnerabilities complicates the remediation process, requiring extensive management and repair efforts by IT teams [19]. For instance, Microsoft, facing 600,000-700,000 cyber attacks daily, invests heavily in network security, with TrickBot likely contributing to these attacks [20].

In October 2020, Microsoft's legal action led to the disabling of TrickBot C2 server IP addresses, prompting the operators to establish new infrastructure and distribute new TrickBot samples [12]. The development of a special component, Anchor, indicates TrickBot's expanding customer base, including nation-state actors [12]. These developments underscore that the complete eradication of TrickBot botnet remains a challenge, continuing to pose significant cybersecurity risks.

V. Defense Solution

Given the longevity of botnets, people have developed various strategies to counter these threats. However, TrickBot continues to evolve, making it challenging to combat. One straightforward solution is to eliminate all harmful botnets from the internet. The method described in "Zero Botnets: An Observe—Pursue-Counter Approach" involves using network data to identify and halt malicious traffic [21]. However, this approach can be resource-intensive and may raise concerns about surveillance techniques. Some nonprofit organizations are working towards this solution for botnets in general.

While effective, this method may raise privacy and data concerns, especially if implemented by a government body. The article acknowledges these issues but suggests that the approach's benefits might outweigh the costs [21]. Companies can address these concerns on an individual basis, tailoring the solution to their specific needs.

For solutions more directly targeting TrickBot, rather than general botnets, various options exist. The CISA and FBI recommend blocking suspicious IP addresses, using antivirus software, and providing social engineering and phishing training to employees [22]. These methods depend on human ability to recognize potential threats and on advanced software capable of handling evolving threats like TrickBot. Training individuals to identify suspicious links or emails is crucial, as is maintaining a security protocol for handling threats or accidental exposure to malware. Minimizing human error is key, as security issues often stem from poor password practices or clicking on suspicious links. Training to identify phishing attacks is particularly important in defending against TrickBot.

Additionally, technical measures can be employed against TrickBot. Implementing Domain Message Authentication Reporting and Conformance (DMARC) can help identify spoofed or altered emails [23], while using MS-ISAC's Albert system can monitor network traffic for malicious activity [24]. Upgrading to SMBv2 instead of SMBv1 can also offer better protection against TrickBot's network propagation modules [23]. Keeping security systems updated and adopting modern security measures are vital in staying ahead of TrickBot. Table II shows defensive solutions and their descriptions.

In summary, defense solutions against TrickBot include using antivirus software, employee training, and implementing additional security protocols. Figure 3 lists all the discussed solutions.

Simple precautions, such as cautious internet browsing and skepticism towards email attachments, can prevent infections like TrickBot. Always update software to fix identified vulnerabilities.

Table II: Defensive solutions and their brief descriptions

Solutions:	**Descriptions:**
Observe-Pursue-Counter	Monitor network traffic
Antivirus software	detect and block malware
Social engineering	Learn social engineering tactics
Phishing Training	Training to identify phishing
Blocking Internet Protocol	Block suspicious activity
DMARC	Report modified emails
MS-ISAC's Albert system	monitor suspicious network
SMBv2	server message blocker

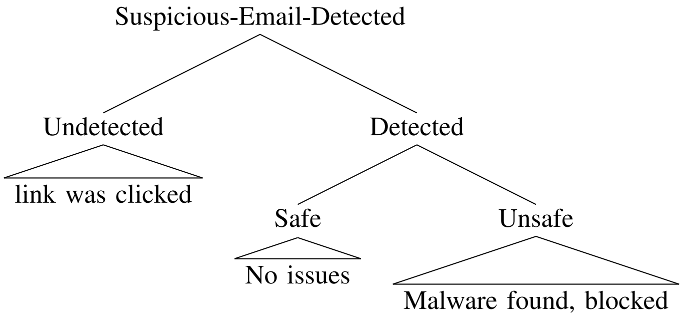


Figure 3: A tree diagram illustrating steps to avoid a botnet [25].

Automation makes it harder to discern malicious from safe emails. TrickBot's extensive email database means messages from these addresses appear trustworthy. Look out for Microsoft Word and Excel files with hidden JavaScript code, or emails mimicking messages from managers. Most of these malicious attachments appear legitimate, contributing to TrickBot's effectiveness. Figure 3 illustrates steps to avoid a botnet.

VI. Conclusion

In conclusion, since its emergence in October 2016, the TrickBot Botnet, a potent banking Trojan, has consistently targeted prominent banks worldwide, including those in North America, Europe, and Australia. Persistently active, TrickBot has infected over 140,000 machines in the last 16 months. Its primary targets are Windows machines, with user data often compromised through phishing emails and other deceptive methods that prompt users to download malicious software. Once a device is infected, TrickBot employs various attack vectors, such as SpearPhishing, Network Vulnerabilities, and Secondary Payloads.

To effectively defend against the TrickBot Botnet, it is crucial to implement a range of strategies including network traffic monitoring, deploying antivirus software for malware detection and blocking, educating on social engineering tactics, phishing attack recognition training, blocking suspicious internet activity, reporting altered emails, monitoring for suspicious network activity, and utilizing server message blocking techniques.

A significant challenge in combating TrickBot is its nature as a network of compromised devices, making complete eradication difficult. This complexity contributes to its longevity and prevalence in the cyber threat landscape. The group behind

TrickBot has progressively enhanced its capabilities, rendering the Trojan increasingly dangerous and resilient. In 2019, TrickBot accounted for 25 percent of all prevalent malware. Its methods of attack continue to evolve, incorporating new tools and techniques to exploit vulnerabilities. The Trojan's stealth, coupled with its ability to compromise entire systems and disguise phishing emails as legitimate, makes detection particularly challenging. With access to approximately 300 million email accounts, TrickBot can distribute seemingly safe emails, further complicating efforts to curb its spread.

References

[1] L. Kessem, "Dyre Straits: Group Behind the Dyre Trojan Busted in Moscow?." https://securityintelligence.com/dyre-straights-group-behind-the-dyre-trojan-busted-in-moscow/.

[2] L. Loeb, "TrickBot Malware Resurrects the Ghost of Dyre." https://securityintelligence.com/news/trickbot-malware-resurrects-the-ghost-of-dyre/.

[3] R. Lakshmananb, "Notorious TrickBot Malware Gang Shuts Down its Botnet Infrastructure." https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html#:~:text=Attributed\%20to\%20a\%20Russia\%2Dbased,was\%20dismantled\%20in\%20November\%202015.

[4] Kaspersky, "What is a botnet?," Mar 2022.

[5] A. G. Ruveyda Celik, "Behavioral analysis of trickbot banking trojan with its new tricks," *International Journal of Technology and Engineering Studies*, vol. 5, no. 3, pp. 95–105, 2019.

[6] B. L. Labs, "A Look Inside The TrickBot Botnet." https://blog.lumen.com/a-look-inside-the-trickbot-botnet/.

[7] A. Culafi, "Trickbot has infected 140,000-plus machines since late 2020." https://www.techtarget.com/searchsecurity/news/252513466/Trickbot-has-infected-140000-plus-machines-since-late-2020.

[8] D. Ruiz, "Trojan.trickbot: Malwarebytes labs," 2018.

[9] D. B. Johnson, "Trickbot trojan takes aim at vulnerabilities in booting process." https://www.scmagazine.com/news/content/trickbot-trojan-takes-dangerous-aim-at-vulnerabilities-in-booting-process.

[10] O. Ozer, "The curious case of a fileless trickbot infection," Apr 2022.

[11] "Latvian national charged for alleged role in transnational cybercrime organization," Jun 2021.

[12] L. Constantin, "TrickBot explained: A multi-purpose crimeware tool that haunted businesses for years." https://www.csoonline.com/article/3600457/trickbot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years.html.

[13] C. P. Blog, "December 2021's Most Wanted Malware: Trickbot, Emotet and the Log4j plague." https://blog.checkpoint.com/2022/01/12/december-2021s-most-wanted-malware-trickbot-emotet-and-the-log4j-plague/.

[14] C. P. P. Releases, "January 2022's Most Wanted Malware: Lokibot Returns to the Index and Emotet Regains Top Spot." https://www.checkpoint.com/press-releases/january-2022s-most-wanted-malware-lokibot-returns-to-the-index-and-emotet-regains-top-spot/.

[15] intel471, "Something strange is going on with Trickbot." https://intel471.com/blog/trickbot-2022-emotet-bazar-loader.

[16] A. S. Gillis, "TrickBot malware." https://www.techtarget.com/searchsecurity/definition/TrickBot-malware.

[17] L. Mathews, "Stealthy TrickBot Malware Has Compromised 250 Million Email Accounts And Is Still Going Strong." https://www.forbes.com/sites/leemathews/2019/07/14/stealthy-trickbot-malware-has-compromised-250-million-email-accounts-and-is-still-going-strong/?sh=2f1037fb4884.

[18] E. Nakashima, "Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election." https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

[19] W. Zamora, "TrickBot takes over as top business threat." https://www.malwarebytes.com/blog/news/2018/11/trickbot-takes-top-business-threat.

[20] N. Goud, "Microsoft to invest $1 billion per year on Cyber Security." https://www.cybersecurity-insiders.com/microsoft-to-invest-1-billion-per-year-on-cyber-security/.

[21] J. Kepner, "Zero botnets: An observe-pursue-counter approach," 2022.

[22] "Alert (aa21-076a)," Mar 2021.

[23] "Blog: Trickbot: Not your average hat trick - a malware with multiple hats," Apr 2021.

[24] "Albert network monitoring," Nov 2021.

[25] P. P. Kundu, T. Truong-Huu, L. Chen, L. Zhou, and S. G. Teo, "Detection and classification of botnet traffic using deep learning with model explanation," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–15, 2022.