SOCIAL ENGINEERING A CHAINED, POTENT ATTACK VECTOR

Siddhant Tiwari
AIT Computer Science Engineering
Chandigarh University
Mohali, India

Neha Varma
AIT Computer Science Engineering
Chandigarh University
Mohali, India

Atharva Barge
AIT Computer Science Engineering
Chandigarh University
Mohali, India

Mr. Yogiraj Bhale
Assistant Professor
AIT Computer Science Engineering
Chandigarh University
Mohali, India

***Abstract*— The "Social Engineering: A Chained, Potent Attack Vector" project demonstrates how attackers bypass traditional security perimeters by exploiting the human element. This multi-stage attack simulation uses a deceptive "lure" (the social engineering component) to trick a user into executing a persistent payload.. This project is designed to analyze common security threats like credential theft (via keylogging), data exfiltration, and remote system compromise, highlighting how even if technical defenses are in place, the human element can be leveraged to compromise an entire system.**

***Keywords*— Social Engineering, Attack Vector, Keylogger, Cybersecurity, Human Vulnerability, Payload.**

I. INTRODUCTION

The evolution of digital interconnectedness has established human trust as a primary, exploitable attack surface in cybersecurity. While conventional security paradigms focus on technical vulnerabilities and network hardening, social engineering exploits the human operator, bypassing technical controls entirely [1], [2]. Traditional, single-vector attacks, such as mass phishing emails, are increasingly mitigated by filtering technologies and user awareness training [3], [4]. In response, threat actors have evolved to deploy Chained Social Engineering, a far more potent vector that sequences multiple, disparate attack modalities to construct a synthetic "chain of trust" and progressively disarm target skepticism [5], [6].

Even with robust defensive postures, chained vectors remain a major barrier to organizational security. These multi-modal attacks exploit the cognitive gaps in human perception rather than software flaws [7], [8]. Numerous studies [9], [11] have highlighted the psychological principles involved, such as trust transference and authority bias. Krol et al. [3], for instance, might be adapted to suggest that attackers who "prime" a target with one channel (e.g., an SMS alert) find that the target is significantly less skeptical of a follow-up on a second channel (e.g., a phone call), perceiving it as verification [10]. Studies on high-pressure environments [7], [12] also show that the introduction of urgency or authority severely degrades a user's ability to detect coordinated deception.

Furthermore, the primary objective of these chained attacks has evolved beyond simple credential theft. They are now the preferred vector for bypassing multi-factor authentication (MFA). Attackers use "vishing" (voice phishing) in conjunction with Adversary-in-the-Middle (AiTM) phishing kits [13], [14], socially engineering the target into approving an MFA push notification or revealing a one-time password (OTP) [11]. Researchers have thus argued for technical controls that are resistant to such social manipulation, such as hardware tokens (e.g., FIDO2) that bind authentication to the origin domain, rendering the psychosocial manipulation ineffective [15], [16].

Growing relevance of chained attacks is shown by their prevalence in high-impact breaches, including Business Email Compromise (BEC) [17], ransomware deployment [18], and targeted supply chain attacks [19], [20]. Creative innovations, such as the use of real-time voice cloning (RTVC) deepfakes [21] and AI-driven pretexting [22], are redefining the threat landscape by automating the creation of highly convincing, personalized attacks at scale.

Still challenging is finding a balance between operational efficiency and security friction. Studies suggest that overly complex verification procedures can discourage users, leading them to seek insecure workarounds [23], [24]. Larger organizational resilience thus depends on developing a socio-technical defense-in-depth model that correlates anomalous events across disparate systems without compromising workflow [25], [26].

Under this framework, the present work aims to investigate the evolving terrain of Chained Social Engineering. It will evaluate the psychological mechanics and technical components of these multi-modal attack vectors and propose approaches for more resilient, correlated defensive systems. Using concepts from present research [1]–[28], this work advances a better understanding of how socio-technical defenses can be tailored to satisfy the rising needs of a secure digital environment against these potent, chained threats.

II. LITERATURE REVIEW

The body of studies on social engineering and human-centric threats underlines how much more crucial holistic, behavior-based defense systems are for safeguarding organizational assets across several communication channels. Underlining the need for more dynamic detection mechanisms, conventional single-vector defenses have repeatedly shown shortcomings to attacks including spear-phishing, pretexting, and business email compromise (BEC), although still rather common [29]. Usually, creating a plausible scenario (e.g., a technical issue) and leveraging a trusted identity (e.g., an IT administrator or executive) [30], social engineering has responded as a primary vector of compromise, greatly bypassing technical security perimeters.

Among the several social engineering tactics, Multi-Modal Attack Chaining and Cross-Channel Pretexting have become rather popular. Based on the principles of cognitive trust transfer, Chained Vectors generate a sequence of interactions across different platforms that validate one another, so highly resistant to user skepticism and standard spam filtering [31]. Operating on a psychological "consistency" paradigm, these attacks allow situations whereby an initial benign contact lowers defenses while a subsequent high-pressure request guarantees payload execution [32]. Replacing less complex methods such as bulk phishing emails, which have been shown to be vulnerable to automated detection and user apathy [33]. These complex chains have evolved into basic components of advanced persistent threats (APTs).

Another major emphasis of security research has been the cognitive vulnerability of the target. Following an exhaustive analysis of many deception techniques, Mouton et al. (2016) [34] concluded that multi-modal stressors find the ideal mix between urgency and authority. Unlike isolated phishing emails, which can be easily ignored or deleted, chained attacks use mediums consumers already trust—such as SMS and voice calls—so reducing scrutiny and preserving strong illusionary legitimacy. Still, detection problems remain particularly in high-volume corporate environments where verifying every communication is impractical—a topic sometimes blamed for inducing "security fatigue" and reducing more general user vigilance [35].

Simultaneously, a big concern now is the automation of pretext creation. Currently, best practices for attackers include maintaining consistency using AI-driven Large Language Models (LLMs) and real-time deepfake voice cloning, which separate the attacker's actual identity from the simulated persona [36]. Moreover, shown to boost attack success rates even in cases of heightened suspicion is the integration of personalized OSINT data including recent transactions, colleagues' names, and internal project codes [37]. This adds still another challenge to human threat detection.

Furthermore obviously basic for modern social engineering solutions is contextual relevance. Research underlines the need of generating pretexts that align with the target's current business context without depending on generic templates, so guaranteeing engagement even in high-security or zero-trust environments where generic phishing would be blocked [38]. In supply chain attacks and among vendors with integrated access to larger networks, this feature is particularly dangerous.

Furthermore, the literature has given Out-of-Band (OOB) Verification great importance as a necessary but sometimes disregarded aspect of anti-social engineering design. Studies reveal that lack of basic, codified verification channels greatly increases the likelihood of successful financial fraud or credential theft [39]. Proposed today to help lower these risks are mandatory callback policies, FIDO2 hardware authentication implementation, and user education on cross-referencing communication sources.

All things considered, the evolution of social engineering technologies points to vectors that are not only psychologically manipulative, resistant to technical filters, able of operating across multiple platforms, but also highly automated. Combining AI-driven content generation with deepfake voice synthesis with multi-stage attack flows—combined with threats to remote workforces—which continue to rise in complexity—represents a major threat landscape development. These advances support the more general drive toward as resilient as they are adaptive defense systems, so ensuring that robust verification policies do not compromise operational efficiency.

III. PRELIMINARY ANALYSIS

Particularly Multi-Modal Pivoting and Cross-Platform Pretexting, Chained Social Engineering vectors—especially are underlined in the growing corpus of research as absolutely necessary for bypassing modern digital security systems. Studies repeatedly show that adding a second communication channel greatly lowers the likelihood of defensive detection even in cases where the initial contact would be flagged as suspicious [40]. Most people agree nowadays that this multi-layered attack approach is the minimum needed basis for compromising high-value targets protected by anti-phishing filters, endpoint detection, and awareness training.

Furthermore underlined in the literature is how generally SaaS-based reconnaissance solutions are valuable, particularly in cross-organizational environments. Thanks to native interaction with platform-specific APIs like Microsoft Graph and LinkedIn Scrapers, studies show that automated reconnaissance tools—built on frameworks like Python Scrapy or Maltego—offer improved targeting precision without triggering alerts [41]. Using open-source intelligence (OSINT) and public relationship mapping guarantees that sensitive hierarchy data is harvested from more general public footprints, so addressing a vital element in contemporary targeting environments.

Apart from vector development, present advancements in Pretext Resilience and Narrative Recovery have attracted particular interest. Studies reveal that although single-vector attacks significantly fail against skeptical users, improperly built chains can unintentionally lead to "narrative collapse" and immediate reporting [42]. Synchronized narrative anchors, establishing authority on a secondary channel (e.g., SMS), and "time-shifting" the attack to non-business hours are suggested best practices that ensure attack continuity and credibility without compromising the illusion of legitimacy.

Moreover, the inclusion of Generative AI (GenAI) into social engineering workflows is clearly a great improvement. By requiring voice cloning, real-time translation, or deepfake-based verification before the target can question the attacker's identity, systems offer another layer of psychological manipulation, so neutralizing defenses presented by voice recognition or skepticism of text-based requests [43]. Emphasizing "verified" personas over anonymous spoofing, these layered attack models closely relate with the exploitation of Zero Trust concepts.

Moreover, repeatedly emphasized in offensive security research is the need of Out-of-Band (OOB) capability for attack systems. Literature shows that depending too much on a single corporate channel (like email) disturbs the attack flow and opens other detection paths. Therefore, particularly in high-security or monitored environments, leveraging personal devices (BYOD) via SMS or WhatsApp—independent of corporate network logging—is considered as absolutely necessary for preserving attack resilience [44]. This OOB capacity ensures ongoing manipulation even in situations when traditional network monitoring would otherwise block the interaction.

Taken together, these findings suggest that the direction of advanced social engineering will be defined by developing complete, target-centered solutions that easily combine strong psychological triggers, reliable narrative recovery, AI-driven impersonation, and platform-agnostic pivoting approaches. The proposed attack taxonomy is well-aligned with these new offensive best practices and offers a strong, readily available, highly potent framework for understanding present human-centric vulnerabilities by including multi-channel support, OSINT integration, deepfake capabilities, and encrypted OOB communication.

IV. COMPARING PROPOSED SOLUTIONS

In our research of quantifying the efficacy of post-exploitation payloads delivered via social engineering, two distinct execution architectures—Design 1, a Standalone Compiled Binary utilizing PyInstaller, and Design 2, a Cloud-Native "Living off the Land" (LotL) script utilizing Google Firebase—were closely investigated. The performance and resilience of both systems were evaluated using criteria including execution environment dependency, network traffic stealth, persistence stability, and forensic footprint.

Design 1 demonstrated superior deployment flexibility through its Bundled Runtime strategy. By compiling the Python payload into a monolithic executable (.exe) using PyInstaller [45], this design eliminates the dependency on a pre-installed Python environment, making it viable for a broad spectrum of Windows targets. The payload establishes persistence via Registry Manipulation, writing directly to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, a technique widely documented in malware persistence taxonomies [46]. Data exfiltration is handled through Direct Socket Communication, posting logs from a local staging file (e.g., %TEMP%\sys_log.dat) to a custom-controlled Command and Control (C2) server.

However, the detection profile of Design 1 proved to be a significant liability. Compiled Python scripts possess distinct headers and signature anomalies that are frequently flagged by Antivirus (AV) heuristics and static analysis engines [47]. Furthermore, the reliance on direct HTTP connections to unknown IP addresses creates a "noisy" network signature, easily blocked by corporate firewalls or identified by Endpoint Detection and Response (EDR) agents as suspicious process behavior.

Design 2 presents a more sophisticated, evasion-centric methodology by leveraging Reputation Hijacking, a core component of "Living off the Land" (LotL) tactics [48]. Instead of a custom C2 server, the payload utilizes the firebase_admin SDK to tunnel traffic through the Google Firebase Realtime Database. This ensures that all exfiltration occurs over encrypted HTTPS (TLS 1.3) channels pointing to a trusted domain (firebaseio.com) [49], blending malicious traffic with legitimate background noise. Design 2 operates on an Asynchronous Queueing model, where keystrokes are buffered in a thread-safe memory queue (RAM only) and pushed to the cloud in bursts, eliminating the disk footprint associated with local file staging.

Persistence in Design 2 is achieved through User-Land Stealth. Rather than modifying the Registry, the script deposits a lightweight batch wrapper (.bat) into the %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup directory. This method requires no administrative privileges and avoids the heuristic triggers associated with Registry modification [50]. The inclusion of a Remote Kill Switch, which triggers os.remove(sys.argv[0]) upon a cloud-based signal, allows for rapid, clean self-destruction.

Still, Design 2's reliance on Interpreter-Based Execution makes major concessions regarding target compatibility. The requirement for a host python environment (or the deployment of a portable embeddable zip) limits the target demographic primarily to developer or administrator workstations. This dependency adds a layer of complexity to the initial "Social Engineering Lure" phase, as the environment must be validated before execution can succeed.

All things considered, the comparison study stresses several advantages and trade-offs included in every design. Perfect for broad-scope campaigns targeting general users, Design 1 excels in providing a "fire-and-forget" executable that runs anywhere but carries a high risk of detection. Design 2 offers a perfect, stealth-oriented solution for high-value targets (HVT), leveraging cloud-native trust anchors to bypass network filtering, yet it requires a specific execution environment. Future studies could look at hybrid models that utilize a lightweight compiled dropper (Design 1) to fetch and execute the cloud-native payload (Design 2) in memory, offering a complete attack solution catered to hardened operational settings.

V. CONCLUSION AND FUTURE WORK

The escalating success rate of social engineering attacks has been reflected in the intense competition among cybersecurity training and threat detection vendors. It also forces the open-source development of human-centric defense mechanisms. These future defense systems will need to be built with reduced deployment time and further user-centric, easily updateable modules.

Particularly concerning AI-driven phishing and deepfake-based vishing (voice phishing), the future of social engineering defense is fast changing in response to developing cybersecurity concerns, the user demand for unobtrusive security protocols, and an increasing focus on organizational resilience. The demand for more flexible, scalable, and context-aware defense solutions keeps driving innovation as the threat landscape gets ever more complicated.

Integration of Artificial Intelligence (AI) and Natural Language Processing (NLP) is a fundamental direction toward the enhancement of the suggested systems. Future iterations of these defense programs can include real-time sentiment and syntax analysis rather than depending just on static blocklists and known-signature detection. This would provide real-time threat monitoring, immediate mitigation should an employee interact with a malicious actor, and seamless multi-channel protection (email, SMS, VoIP). Using end-to-end encrypted cloud-based analysis services can help developers improve scalability and detection accuracy without incurring large on-premise infrastructure expenses. Faster analysis procedures and lower latency made possible by the elastic computing capability of the cloud help to improve the user experience without compromising data privacy.

Future versions should also give modular architecture a priority. Development time for new detection features and adaptations will be much reduced by security frameworks constructed with easily interchangeable modules—for payload analysis, psychological trigger detection, or communication channel monitoring. This modularity not only facilitates a quick reaction to new manipulation techniques (e.g., forthcoming real-time video deepfakes) but also helps open-source communities to contribute and grow the defense platform cooperatively more easily.

Moreover, employee acceptance and vigilance depend much on additional improvements in Quality of Life (QoL) regarding security training. These comprise better user interfaces for reporting suspicious activity, gamified learning systems to reduce fatigue, customizable training intervals, and smart notifications depending on user risk profiles or recent attack trends. Future uses should stress accessibility to guarantee that security awareness flows are equally simple for non-technical staff and should include localization support for global workforces.

Emerging standards like Zero Trust Architecture (ZTA) and identity verification protocols allow one to also improve the integration of anti-social engineering measures. Future systems can rely less on implicit trust by using such standards, hence shifting toward a safer and more skepticism-based verification model. Further enhancing security and simplicity, multi-modal verification mixed with cryptographic attestation would let users verify the identity of a requester without awkward manual intervention or disrupting business workflows.

Finally, models of adaptive behavioral security provide a fascinating horizon. These models would let the defense system dynamically change its needed degree of scrutiny depending on contextual cues including communication urgency, request anomalies, or behavioral deviations. Systems can more wisely balance usability and vigilance by doing this, therefore enforcing tougher verification steps only when high-risk psychological triggers are detected.

Ultimately, the scene of social engineering defense is about to undergo major change. The future generation of protection systems will be defined by AI integration, modular design, user-centric awareness updates, acceptance of Zero Trust principles, and the application of adaptive behavioral mechanisms. The solutions covered in this paper provide a basic framework that can be developed to satisfy the security and usability issues of the future, therefore benefiting a broad spectrum of stakeholders from individual users to massive corporate infrastructure systems.

Acknowledgment

Authors would like to express their sincerest gratitude to Professors from Chandigarh University for their inputs and revision suggestions on earlier versions of this paper. Any and all errors are our own and should not tarnish the reputation of these esteemed persons.

References

[1] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social Engineering: The Human Side of Hacking," *Computers & Security*, vol. 59, pp. 186–209, 2016.

[2] S. Pfleeger and D. Caputo, "Leveraging Behavioral Science to Mitigate Cyber Security Risk," *Computers & Security*, vol. 31, no. 4, pp. 597–611, 2012.

[3] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, "'They brought in the horrible key ring thing!' Analysing the Usability of Two-Factor Authentication in UK Online Banking," in *Proc. Workshop on Usable Security (USEC)*, 2015.

[4] M. Junger, L. Montoya, and F. Overink, "Priming and Warnings: The Influence of Security Education on Phishing Susceptibility," *Computers in Human Behavior*, vol. 73, pp. 102–110, 2017.

[5] D. Aniagolu, "Multimodal AI: A Whole New Social Engineering Playground for Hackers," *Security Boulevard*, Oct. 2025. [Online].

[6] A. Herzberg and A. J. Y. Bar-Noy, "The Trust Chain: A Mathematical Model for Multi-Modal Authentication vectors," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 201–215, 2024.

[7] R. Cialdini, *Influence: The Psychology of Persuasion*, New York: Harper Business, 2006.

[8] J. R. B. Workman, "Gaining Access with Social Engineering: An Empirical Study of the Threat," *Information Systems Security*, vol. 16, no. 6, pp. 315–331, 2007.

[9] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed. New York: Wiley, 2018.

[10] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in *Proc. CHI Conference on Human Factors in Computing Systems*, 2010.

[11] M. G. Kovacs and S. R. Lui, "The Psychology of MFA Fatigue: Exploiting the Push Notification," *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, pp. 112–128, 2023.

[12] A. Vishwanath, "The Impact of Authority and Urgency on Phishing Susceptibility," *Communication Research*, vol. 43, no. 2, pp. 179–203, 2016.

[13] Microsoft Security Threat Intelligence, "The Rise of AiTM (Adversary-in-the-Middle) Phishing Kits," *Microsoft Security Blog*, 2023.

[14] Palo Alto Networks Unit 42, "Hybrid Vishing and Phishing Campaigns: A 2024 Retrospective," *Unit 42 Threat Research*, 2024.

[15] Yubico, "Phishing-Resistant Authentication: The FIDO2 Standard," *Yubico Technical Whitepaper*, 2023.

[16] W. A. Khan, "Domain Binding and the End of Credential Harvesting," *ACM Computing Surveys*, vol. 55, no. 3, 2023.

[17] Federal Bureau of Investigation (FBI), "Business Email Compromise: The $43 Billion Scam," *Internet Crime Complaint Center (IC3) Report*, 2023.

[18] Mandiant, "Ransomware Initial Access Vectors: The Shift to Social Engineering," *Mandiant M-Trends Report*, 2024.

[19] S. Gupta and R. S. Sandhu, "Supply Chain Social Engineering: The Island Hopping Technique," *IEEE Security & Privacy*, vol. 21, no. 4, pp. 34–42, 2023.

[20] ENISA, "Threat Landscape for Supply Chain Attacks," *European Union Agency for Cybersecurity*, 2023.

[21] T. Nguyen, "Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments," *MDPI Computers*, vol. 13, no. 2, 2025.

[22] FPT IS, "Weaponizing Agentic AI for Social Engineering Attacks," *FPT Insight Report*, May 2025.

[23] A. M. Sasse and I. Smith, "The Usability-Security Trade-Off: Users as the Weakest Link or the Scapegoat?" *IEEE Security & Privacy*, vol. 18, no. 6, 2020.

[24] NIST, "Security Fatigue and Shadow IT: Why Users Bypass Controls," *NIST Cybersecurity Insights*, 2022.

[25] A. Alseadoon, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Towards Effective Mitigation Strategies," *IEEE Access*, vol. 11, pp. 15200–15220, 2023.

[26] Splunk, "Correlating Behavioral Anomalies: The SIEM Guide to Social Engineering," *Splunk Research*, 2024.

[27] Gartner, "Predicts 2025: Identity and Access Management in the Age of AI,"

Gartner Research, 2024.

[28] Forrester, "The Zero Trust Model and the Human Element," *Forrester Reports*, 2024.

[29] F. Mouton, M. M. Malan, and H. S. Venter, "Social Engineering Attack Framework," *Information Security for South Africa*, 2014.

[30] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley, 2002.

[31] A. Herzberg and A. J. Y. Bar-Noy, "The Trust Chain: A Mathematical Model for Multi-Modal Authentication Vectors," *IEEE Transactions on Information Forensics*, 2024.

[32] R. B. Cialdini, *Influence: The Psychology of Persuasion*, Harper Business, 2006.

[33] Z. Benenson, F. Gassmann, and R. Landwirth, "Unpacking Spear Phishing Susceptibility," *Financial Cryptography and Data Security*, 2017.

[34] F. Mouton, L. Leenen, and H. S. Venter, "Social Engineering: The Human Side of Hacking," *Computers & Security*, vol. 59, 2016.

[35] B. Reinheimer et al., "An Investigation of Phishing Awareness and Education over Time: When Instructions Wear Off," *Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[36] S. Gupta, "AI-Enabled Social Engineering: The Rise of Deepfake Vishing," *Journal of Cybersecurity Trends*, 2025.

[37] J. R. Workman, "Gaining Access with Social Engineering: An Empirical Study of the Threat," *Information Systems Security*, 2007.

[38] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd Edition, Wiley, 2018.

[39] S. Pfleeger and D. Caputo, "Leveraging Behavioral Science to Mitigate Cyber Security Risk," *Computers & Security*, 2012

[40] Z. Benenson, F. Gassmann, and R. Landwirth, "Unpacking the Multi-Modal Threat: Why Single Channel Defense Fails," *ACM Transactions on Privacy and Security*, vol. 24, no. 2, 2024.

[41] J. R. B. Workman and D. A. Cain, "Graph API Exploitation: Mapping the Corporate Hierarchy for Precision Targeting," *Journal of Digital Forensics & Incident Response*, 2025.

[42] S. Vishwanath, "Narrative Collapse: Measuring the Resilience of Social Engineering Pretexts," *Computers in Human Behavior*, vol. 92, pp. 301–315, 2023.

[43] T. Nguyen and A. Verma, "The Deepfake Handshake: Bypassing Voice Biometrics in Social Engineering," *IEEE Security & Privacy*, vol. 23, no. 1, 2025.

[44] P. Kumaraguru, "BYOD as a Backdoor: Leveraging Personal Channels for Corporate Compromise," *MIS Quarterly*, vol. 48, no. 3, 2024.

[45] M. Cortese et al., "PyInstaller: Freezing Python Applications," *PyInstaller Documentation*, ver 6.3, 2024.

[46] MITRE ATT&CK, "Persistence: Registry Run Keys / Startup Folder (T1547.001)," *MITRE Corporation*, 2024.

[47] S. Venkatesan, "Static Analysis of PyInstaller Generated Malware," *SANS Institute InfoSec Reading Room*, 2022.

[48] Symantec Threat Intelligence, "Living off the Land: A Survival Guide for Defenders," *Broadcom Software*, 2023.

[49] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," *RFC 8446*, Internet Engineering Task Force, 2018.

[50] CrowdStrike, "Hunting for Persistence in User-Land Startup Folders," *CrowdStrike Adversary Universe Report*, 2024.