An Actor-Network Theory Analysis of the SolarWinds Orion Hack

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Zachary Lieberman

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Benjamin Laugelli, Department of Engineering and Society

Introduction

On March 25, 2021, SolarWinds released the software update Orion Platform 2020.2.5 which was downloaded by over 18,000 users. However, these users were unwillingly downloading a malicious piece of software that was stealthily injected into the product which gave the hackers access to the client's data. Although no malicious action was made upon that data, the current understanding is that "one of the worst data breaches ever to hit the US government" has led to a series of other attacks such as targeting 3,000 email accounts of over 150 federal agencies in May 2021 (Disis & Mahmood, 2021).

Blame has been placed upon SolarWinds for poor password protection, heeding cybersecurity advise, and limited spending on security. These are all accurate depictions of the factors that led to the attack; however, these interpretations fail to address the sociotechnical factors that caused this breach. The roles of money, complacency, and SolarWinds' clients played a significant role in the build up of this hack and thus should be held in consideration. Limiting the responsibility to just SolarWinds allows only a partial understanding of the situation and readers will have a lack of understanding of all the sociotechnical factors that took place in this large-scale hack.

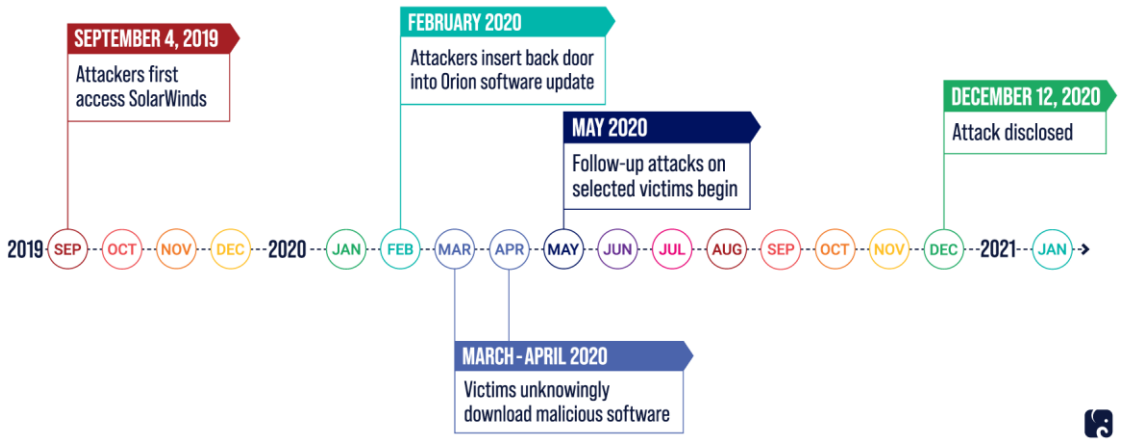
I will outline how the SolarWinds Orion attack was a result of the technical and non-technical factors of SolarWinds' monetary mindset, reluctance to invest in security, and their users' impact. I will use the Actor-Network Theory (ANT) as the framework for this analysis in order to accurately portray the roles that each factor played in this event. ANT is used to correlate a technology network through its various actors in order to discover a failure in that system. My analysis of the SolarWinds Orion attack will rely on primary sources stemming from

various press releases, analyses of the event and its effects, and financial data reflecting the monetary effects of the intrusion.

Background

The SolarWinds Orion software is a collection of information technology (IT) products that provide network, IT operations, and security tooling to government and commercial companies for their organizations. In December 2020, cybersecurity firm FireEye discovered that they had been hacked by a Russian entity through malware linked to SolarWinds Orion. The hackers gained access to SolarWinds' update servers and attached a remote access backdoor into the system that was downloaded by 18,000 clients including at least 9 federal agencies and top private companies such as Microsoft and Cisco (Ernst, 2021). The economic and technological damage from the intrusion is expected to be significant and long-lasting, with estimates suggesting it could cost up to $100 billion to address. This attack has been categorized as a supply-chain operation as the hackers used suppliers of IT, SolarWinds, to access privileged information within their clients' networks (Willet, 2021).

Figure 1: SolarWinds Operation Timeline



Note. SolarWinds Orion operation timeline from federal investigation.

Literature Review

There have been several scholarly pieces outlining the causes, potential impact, and suggested actions as a result of the SolarWinds hack. Some experts suggest that the attackers exploited vulnerabilities in SolarWinds' software supply chain, while others believe that the attack was carried out by a state-sponsored group. These papers also discuss potential solutions for preventing similar attacks, such as improving supply chain security, implementing stronger access controls, and increasing transparency and information sharing between organizations. However, what they fail to encapsulate is the failure of all of the actors within the network who each respectively impacted this widespread attack.

In *Lessons of the SolarWinds Hack*, Marcus Willett argues that a better understanding and mitigation of supply-chain attacks could have prevented the widespread damage of internet and communications technology (ICT) to thousands of companies as a result of the SolarWinds hack. Willett asserted two different potential motives behind the attack, citing that this was a supply-chain operation using the supplier of information technology, SolarWinds, to gain access to adjacent clients' networks to extract data. However, he also provided another interpretation that this could have been a targeted attack towards specific targets utilizing the vulnerable software to penetrate the US cyberspace and cloud service providers. Willett emphasized SolarWinds' lax security practices that allowed the intruders to hide within the security update and the due diligence required upon both the vender and the recipients to ensure secure networks and user data (Willet, 2021). He employed much of the blame and potential solutions of the attack upon the government to create new legislation and sanctions upon venders and other nation states, but lacked the equitable societal failures that contributed to this incident.

Peisert et al. add to these claims by offering their own interpretations and reflections of the SolarWinds hack each with differing reasoning and solutions. Bruce Schneier further explains that SolarWinds' poor security practices were a result of underspending on security and an uptick in the outsourcing of software development to other firms to improve profitability over product safety. This even caused the company's cybersecurity advisor to quit over the company not accepting his basic security recommendations. As explained by Hamed Okhravi, the additional tooling added to each software update adds a new attack surface for actors to enter the system without adequate security measures equally applied. The authors agree on the fact that there was a failure of an organizational comprehensive approach to security that applies not to just technical changes but organizational and educational changes that would improve security awareness and resilience on a wide scale (Peisert et al., 2021).

The scholarly article written by Marcus Willett highlights the importance of SolarWinds' supply-chain attacks in the US cyberspace while providing the cause and effects of their actions and inactions. Peisert et al. introduces SolarWinds' monetary decision making that neglected adequate security measures and the necessary inclusion of new security measures for new tooling in a software update. While these scholars explain the technological causes and effects of the SolarWinds hack, I will further identify the factors that caused the software to fail using Actor Network Theory (ANT).

Conceptual Framework

My analysis of the SolarWinds hack utilizes the science, technology, and society (STS) framework ANT to describe the relevant parties associated with the software's failure in 2020. This concept will allow me to analyze the individual entities that contributed to the intrusion of the malware and its spread within the US cyberspace. ANT is used to analyze the various

resources or actors who comprise a technical network. In this network, there are both human and non-human actors who enter the network through a process called translation. In translation, there are four distinct phases that outline the formation and maintenance of the network: problematization, interessement, enrolment, and mobilisation (Callon, 1984). Problematization occurs when a network builder determines that there is a problem or objective that certain actors must achieve. Interessement involves the network builder recruiting those human and non-human actors into the network as heterogeneous or no more influential than another and their power is kept to the extent of the network. Enrolment, the main focus of this paper, involves network builders assigning those actors to specific roles and more importantly requiring the actors in the network to accept and uphold these roles to the best of their ability. Finally, the mobilisation phase requires the network builder to ensure their position as a representative for the other actors (Callon, 1984).

The analysis of a network using ANT is important to discover where and how actors in a network caused a technology to fail. It is also imperative to outline the various factors that caused the failure drawing from primary sources to interpret them. In the following paper, I will use Actor-Network Theory to identify key actors within the sociotechnical network and how various factors in this network caused the SolarWinds Orion hack to take place.

Analysis

Building a Network

In the 1990s, all software and servers were based within the organization and network of each specific company or on premises. Yet starting in 1994, the dot.com boom allowed for alternative organizational layouts and brought forth the creation of various IT management

companies such as Salesforce in 1999 (Fryer, 2023). These IT management companies developed a different way to sell software by providing their tools and services as a monthly subscription or software as a service (SAAS).

SolarWinds, also starting in 1999, began developing network monitoring software and following multiple acquisitions focused on a SAAS framework as their software development modal. In 2017, SolarWinds released their SAAS product Orion which allowed other organizations to utilize various tools for network management, infrastructure management, application performance management, and database performance management (*Orion Platform*, 2023). SolarWinds Orion subscribers could pick and choose each management tooling to utilize the entire suite or a particular selection of desired tools. SolarWinds began the first stage of translation, problematization, by identifying the changing landscape from on premise software to SAAS. They understood the hassle of each organization idealizing, developing, and maintaining their own software and servers with the goal of a simplified subscription service.

SolarWinds then began to recruit organizations to use their products. At the time of the attack, they had garnered over 300,000 users of their products with the Orion platform maintaining 33,000 of that total including 425 of the Fortune 500 companies. These companies are also made up of highly secure organizations including 9 federal agencies, major defense contractors such as Boeing, and the Los Alamos National Laboratory who develop sensitive nuclear weapons (Sanger et al., 2020). This period of interessement drew in these companies and agencies and aligned their interests to the problem definition SolarWinds sought to solve. This amounts to a large recruitment from the federal government with the Department of Defense (DOD) spending over $2.0 million and the Department of Veterans Affairs spending $2.8 million

in 2020 (*Federal Awards*, 2020). SolarWinds was able to recruit a base that relied heavily on their software in all realms of American and international industries.

Enrolment Failure Leads to Attack

The point of failure was reached upon the network's period of enrolment where various actors were unable to accept and perform their duties to achieve the goal of a secure, functioning management IT service. This begins with the failure to follow an important policy in the United Nations Cyber Norms outlined by the UN General Assembly in 2015:

> States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (Hogeveen, 2015).

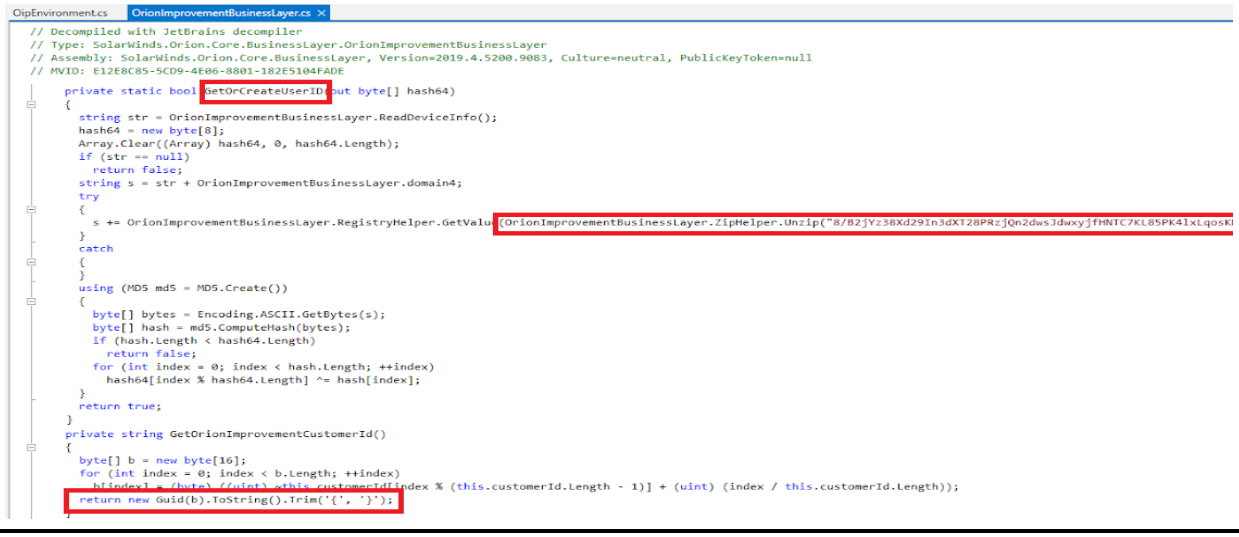
I argue that this policy on security efforts of Internet and Communications Technology (ICT) accounts for the failures of not just SolarWinds in this attack but the failures of all of the relevant actors in this network. The actors within this network held the same amount of power in regards to the success or failure of the primary objective which will be demonstrated by the primary sources I discuss throughout the rest of the paper.

The relevant actors at SolarWinds neglected their obligatory duties to control the supply chain network by minimizing security practices and their recognition of outside adversaries within the system. The top of SolarWinds' organization consisted of ownership groups from private-equity firms Silver Lake and Thoma Bravo, two firms that are 'known for extreme cost-cutting' (Schneier, 2021). The results of severe cost-cutting were detrimental to SolarWinds as they were known to have subpar security for their products to which former CEO Kevin B.

Thompson frequently avoided discussing (Sanger et al., 2021). This history of a lackluster support for adequate security measures led to the upsurge in outsourcing of their software engineering to overseas programmers. Spreading out the workload to external personnel increases the risk of security vulnerabilities which lead to the exploit in the network. Between 2011 and 2014, SolarWinds acquired 12 companies who made threat monitoring software, email security, database security monitoring, and IT support tools. This allowed SolarWinds to become a product that had all of the relevant IT management tools a client would want with a lacking in quality and security (Stoller, 2021). Yet again, SolarWinds winds up in a situation where they add more and more to their product space without adequately protecting these resources accounting for an inevitable failure of the technical network.

The update server for SolarWinds' network management software was left with an extremely guessable password "solarwinds123" which is pointed to as the intrusion point for the hackers (Schneier, 2021). According to ReversingLabs' analysis of the attack, this access allowed the perpetrators to attach a malicious backdoor into the software's source code which was compiled, digitally signed, and distributed to their clients (Peričin, 2020).

Figure 2: Attacker Changes SolarWinds Source Code



As seen in the figure above, the attackers changed the source code to include a process that would add a new user id to the system granting them access with a seemingly normal function of "Orion Improvement Business Layer." This is shown in the second red box where the perpetrators unzipped the malicious code onto the server which is much different than the function's intended purpose of creating a new user ID. The immense level of sophistication on the adversary's part is outstanding with the congruency of the syntax, naming structures, and functionality, however the backwards approach in security allowed for this to be placed within the update server. This critical error also shows how SolarWinds failed to perform their duty as network builder by negligently allowing the other actors within the network to download software detrimental to their technological goal.

I have argued that SolarWinds failed to accept and perform their duties as the network builder for their Orion software by outsourcing software engineering work, reckless acquisitions, and neglectful security measures. Alternatively, opponents to this view argue that attacks, especially from large nation states, are inevitable due to their sophistication and financial backings. Threat actors are able to work anonymously due to the complex structure of the internet, difficulties of operating international legal policies, and the ability to hide and work from virtually anywhere (McKenzie, 2017). Even if the United States is able to determine a perpetrator, they are frequently unable to show their proof of their findings due to the classified sources and methods used. This makes it fairly difficult to charge the threat actors and allows them to continue to commit more attacks. However, SolarWinds' monetary choices displayed a direct correlation to their vulnerability of an attack. Limiting spending on security and safe cybersecurity practices led to a $3.164 million uptick in spending in Q4 2020 and $10.163 million in Q1 2021 spending for Cyber Incident costs "to investigate and remediate the Cyber

Incident, and legal and other professional services related thereto, and consulting services (*SolarWinds Corporation Quarterly Report*, 2020/2021)." Rather than protecting their products, SolarWinds decided to wait until an attack occurred to secure their network and implement serious time and money into their cybersecurity.

The actors in the public and private sectors also had an impact in the failure of this network by allowing too much access to their network and not properly vetting SolarWinds tools. The federal government invested heavily into SolarWinds' products due to the fact that they are unable to modernize their IT infrastructure on premises. By letting a private company like SolarWinds take control of their IT management, they are unable to keep tabs on them for cybersecurity related threats and thus are blindsided in these matters. The US Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, said following the attacks that the US had to choose to have "privacy and security" by limiting their visibility into private company's networks (Neuberger, 2021). This creates a massive liability for the federal government as they are unable to keep tabs on the products they invest in and the products that have access to their systems. As said by the Defense Innovation Board in 2019, the DOD's military advantage lies in their software advantage (McQuade & Murray, 2019). This software advantage is diminished if they are unable to monitor a penetration in their system as they needed a private company, FireEye, to inform them.

As one of the private companies hit with this attack, Microsoft also utilized the platform that eventually granted access into their network and databases. Their email accounts used by millions, including the government, were divulged to the perpetrators and was the source of future attacks. The Nobelium group targeted 3,000 Microsoft email accounts in May 2021 and it is believed that the source of this issue stemmed from the SolarWinds Orion hack (Disis &

Mahmood, 2021). The hackers were able to send fake emails or phishing emails that allowed malicious backdoors to be placed on the innocent users who clicked on the link. Microsoft claimed that there were no vulnerabilities within their system, but allowing the intrusions of the SolarWinds attack is a clear social vulnerability within their system. Following the SolarWinds attack, Microsoft put out a statement calling for the sharing of information and analysis regarding threat intelligence mostly from the US government (Smith, 2020). However, neither the US government nor Microsoft was able to determine that intruders had been within their systems. Microsoft and the other private companies hit in the attack failed to protect their own networks and products by giving SolarWinds the access they did.

Conclusion

Using the framework of Actor-Network Theory, I depicted how the SolarWinds Orion attack was a result of many technical and non-technical factors within the IT Management platform network. This allowed me to describe with the concept of translation how the network was built in the problematization phase, recruitment of users to the network in the interessement phase, and the failure that transpired in the enrolment phase. The event that occurred was caused by both technical and non-technical elements, including SolarWinds' financial decision making, their reluctance to invest in security, and the impact of their users.

By highlighting both the social and technological factors that brought about the failure of this network, readers will have a more comprehensive understanding of the incident and future large-scale attacks. Rather than just discussing SolarWinds involvement in this attack, the additional actors showcase the interconnectivity of the complex network and how those connections broke in this failure. The factors involved in this incident are not novel, so developing an understanding of their impact can be applied to further analysis in past and future

attacks. The present and future landscape of cybercrime can have drastically different threat actors with AI and ransomware appearing much more prevalently, but recognizing these factors would hopefully help engineers develop more solutions to resolve the mistakes made in the past.

Word Count: 3105

References

Brandom, R. (2020, December 15). *Solarwinds hides list of high-profile customers after devastating hack.* The Verge. Retrieved March 2, 2023, from https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised

Brewster, T. (2020, December 15). *DHS, DOJ and DOD are all customers of Solarwinds Orion, the source of the huge US government Hack.* Forbes. Retrieved March 2, 2023, from https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=2860d5b025e6

Callon, M. (1984). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954x.1984.tb00113.x

Disis, J., & Mahmood, Z. (2021, May 28). *Microsoft says Solarwinds hackers have struck again at the US and other countries | CNN business*. CNN. Retrieved March 4, 2023, from https://www.cnn.com/2021/05/28/tech/microsoft-solarwinds-russia-hack-intl-hnk/index.html

Federal Awards. USAspending.gov. (n.d.). Retrieved March 2, 2023, from https://www.usaspending.gov/search/?hash=0648d41dc5c8ebe1762a360a1342a7a3

Fryer, V. (2023, February 15). *The History of SaaS: From Emerging Technology to Ubiquity*. BigCommerce. Retrieved March 2, 2023, from https://www.bigcommerce.com/blog/history-of-saas/

Fung, B. (2021, May 28). *Microsoft says Solarwinds hackers have struck again at the US and other countries | CNN business*. CNN. Retrieved March 3, 2023, from https://www.cnn.com/2021/05/28/tech/microsoft-solarwinds-russia-hack-intl-hnk/index.html

Hogeveen, B. (2015). *The UN Norms of Responsible State Behaviour in Cyberspace*. Australian Strategic Policy Institute. Retrieved March 3, 2023, from https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

McKenzie, T. (2017, January 2). *Is cyber deterrence possible?* Is Cyber Deterrence Possible? Retrieved March 3, 2023, from https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

McQuade, M., & Murray, R. (2019). Software Is Never Done: Refactoring the Acquisition Code For Competitive Advantage. SWAP Executive Summary 2019. Retrieved March 2, 2023, from https://media.defense.gov/2019/May/01/2002126690/-1/-1/0/SWAP%20EXECUTIVE%20SUMMARY.PDF

Neuberger, A. (2021, February 17). *Press briefing by Press secretary Jen Psaki and deputy National Security advisor for cyber and emerging technology Anne Neuberger*. The White House. Retrieved March 3, 2023, from https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/

Orion platform. SolarWinds. (n.d.). Retrieved March 2, 2023, from https://www.solarwinds.com/orion-platform

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the Solarwinds incident. IEEE Security & Privacy, 19(2), 7–13. https://doi.org/10.1109/msec.2021.3051235

Peričin, T. (2020, December 16). *Sunburst: The next level of stealth*. ReversingLabs. Retrieved March 2, 2023, from https://www.reversinglabs.com/blog/sunburst-the-next-level-of-stealth

Sanger, D. E., Perlroth, N., & Barnes, J. E. (2021, January 2). *As understanding of Russian hacking grows, so does alarm*. The New York Times. Retrieved March 2, 2023, from https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Sanger, D. E., Perlroth, N., & Schmitt, E. (2020, December 15). *Scope of Russian hacking becomes clear: Multiple U.S. agencies were hit*. The New York Times. Retrieved March 2, 2023, from https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Schneier, B. (2021, February 23). *Why was Solarwinds so vulnerable to a hack?* The New York Times. Retrieved March 2, 2023, from https://www.nytimes.com/2021/02/23/opinion/solarwinds-hack.html

Smith, B. (2020, December 20). *A moment of reckoning: The need for a strong and global cybersecurity response*. Microsoft On the Issues. Retrieved March 3, 2023, from https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Solarwinds announces fourth quarter 2020 results. SolarWinds Corporation Quarterly Report Q4 2020. (2020, December 31). Retrieved March 3, 2023, from

https://s22.q4cdn.com/673701899/files/doc_financials/2020/q4/SWI-2020.12.31-EX99.1.pdf

SolarWinds Corporation Quarterly Report Q1 2021. Q1'21 results. (2021, March 31). Retrieved March 3, 2023, from https://s22.q4cdn.com/673701899/files/doc_financials/2021/q1/SolarWinds-Q1'21-Earnings-Call-Presentation.pdf

Stoller, M. (2021, January 3). *How to get rich sabotaging nuclear weapons facilities*. How to Get Rich Sabotaging Nuclear Weapons Facilities. Retrieved March 3, 2023, from https://mattstoller.substack.com/p/how-to-get-rich-sabotaging-nuclear

Willett, M. (2021). Lessons of the Solarwinds hack. *Survival*, *63*(2), 7–26. https://doi.org/10.1080/00396338.2021.1906001