Joseph Murphy
Prof. Levkowitz
Internet and Web Systems I
December 1st, 2022

Security Strength of Open-source software

With the rise of more software breaches, how secure are open-source programs in actuality? Does the risk outweigh the reward? “Global attacks increased by 28% in the third quarter of 2022 compared to the same period in 2021. The average weekly attacks per organization worldwide reached over 1,130” (1). Open-source software is not anymore insecure than its counterpart, proprietary software. Actually, open-source software can be more secure and well maintained due to a variety of reasons. Open-source software has many different people that are viewing the code that allows bugs to be exposed faster than if it was closed source code; also, Open-source software has a great community that helps each other out. Most of the major recent breaches were actually associated with proprietary software, so it is important to know why this is and what this means for you and your organization. There are times where proprietary software is the better tool to use. It is also important to know how many of these breaches come into play and how to protect one’s code and organization from them. Open-source software is not any less secure than proprietary software and has great benefits over proprietary software as well.

Open-source software is “software with source code that anyone can inspect, modify, and enhance” (2). Open-source software is also free to use. Proprietary software is software that is developed and maintained by an organization and costs money to use. The affordability and ease of use is a factor that leads many organizations to adopt and use open-source software, especially in the infancy of their organizations. However, are these organizations opening themselves up to breaches by using open-source software? The answer to that is no, open-source software is not any less secure than proprietary software and might even be more secure due to a variety of reasons. These reasons include the Open Source Community, attack frequencies, and lack of side effects in the code (3). It is also very important to view a couple historic breaches to see how they came about and what can be learned and taken away from them. Looking into the recent SolarWinds breach, we will be able to see how a “once-trusted cybersecurity solution without any open-source code was brought to its knees by unknown actors causing widespread unauthorized access to vast amounts of our Federal Government’s most sensitive data.” (3). We will also look into recent Open-source software breach that weaponized PuTTY, KiTTY, TightVNC with code that installs malware on the end user’s environment. It is important to analyze the similarities and differences of these two breaches in order to learn how to make your organization as secure as possible and pick the right software to use in your own applications. Lastly, we will note the differences and reasons to pick open source vs proprietary software if you are an individual or organization. “When compared simply to the code itself without any additional tools, Proprietary Code is no more secure than open source. By contrast, many would argue that open-source Code is more secure due to a faster fix/patch/update cycle and the pervasive access to source code (Clarke, Dorwin, and Nash, n.d.)” (3).

In early 2020, SolarWinds was breached without them knowing. SolarWinds had a product called Orion that was a monitoring and management tool for large organizations. Some of these organizations were branches of the United States government. A Russian intelligence service was able to modify a routine software update that SolarWinds put out. Organizations received the notice that a new software update for the Orion platform was available, so they logged into the company’s secure website, downloaded the update like they had done countless times in the past, and then ran the update like

they have always done. And for almost a year no one knew that they had just completely compromised themselves. That is one major problem with proprietary software, organizations believe it is secure and don't do any due diligence themselves proving it. Over eighteen thousand customers downloaded and installed this routine software update. These companies included "Microsoft, Intel and Cisco; the list of federal agencies so far includes the Treasury, Justice and Energy departments as well as the Pentagon"(4). These are massive organizations that the Russian Intelligence Service was able to compromise and had the ability to not only steal data, but to alter and destroy it as well. The SolarWinds breach was so devastating because of the tool it was used on. Orion had access to almost everything on these organization's networks. The attackers were able to "modify sealed software code, created a system that used domain names to select targets and mimicked the Orion software communication protocols so they could hide in plain sight. And then, they did what any good operative would do: They cleaned the crime scene so thoroughly investigators can't prove definitively who was behind it" (4). Another issue is that most intrusion detection and prevention tools only work on known threats, thus leaving the organizations open to zero-day attacks like the SolarWinds attack. What made the SolarWinds attack so unique is that it was a supply chain attack, the first major one of its kind. The attackers are always evolving and learning new tricks and ways to attack organizations. They realized they couldn't get into these organizations like FireEye or the CIA, but they didn't need to breach them directly to get access in their organizations. If they could attack the supply chain earlier on before it ever reaches the end organizations, they would have an untouched path into these organizations. As of today, there are still "many companies who are still staunchly anti-open source believing that Proprietary Code is more secure. Despite the opposing views in this debate, one fact remains: 96% of applications use Open Source Code, and 80% of the code in the Software Supply Chain is from open source" (3). Those organizations who chose to use SolarWinds over an open source solution thought they were protecting their organizations from a breach, but they just opened the front door and installed the malware themselves.

This is not to say that open-source software does not have its own vulnerabilities and breaches. No code is perfect and impenetrable. A recent open-source software breach that happened was conducted by a threat actor group called Lazurus. This group has been "lacing PuTTY and other legitimate open source applications with highly encrypted code that ultimately installs espionage malware"(6). These attacks started how most breaches start, through social engineering attacks. They created fake LinkedIns, reached out to targeted individuals and began conversing with them and getting them to believe they were trusted allies. One of the most important things to know in CyberSecurity is that the weakest link is, and will always be, humans. You can build the most secure house ever built, but it does no good if someone leaves a door open. Lazurus then gets these targeted individuals to install compromised versions of open-source software like PuTTY that has "code that installs the same espionage malware, which Microsoft has named ZetaNile … The Trojanized PuTTY and KiTTY apps Microsoft observed use of a clever mechanism to ensure that only intended targets get infected and that it doesn't inadvertently infect others. The app installers don't execute any malicious code. Instead, the ZetaNile malware gets installed only when the apps connect to a specific IP address and use login credentials the fake recruiters give to targets'' (6). Once these hackers have successfully connected to the malware, they can install additional malware on the device and have full access and control over these devices. It is important to note that these breaches only are successful because users install the wrong version of the open-source software. If they went to putty.org and downloaded PuTTY, they would not have been compromised. One issue with open-source software is that anyone has access to it and can edit it to make it their own and share out the malicious new software.

Open-source software has benefits that make it even more secure than proprietary software. These reasons include the Open Source Community, attack frequencies, and lack of side effects in the code. One major benefit of open-source software is that it is free. By using open-source software you can take the money you would have used to purchase proprietary software and use it to strengthen your organization's security posture. Another benefit is the quickness of security fixes. When "proprietary software vendors fix security flaws, they must validate it and get it into a release or patch. This process could take up to a year or more in the worst case. In some cases, the company may decide not to fix the flaw at all. In the Open Source Community, however, end users could apply a fix as soon as it is implemented" (3). Open-source software is more agile than proprietary software and can be edited and changed instantly allowing for a better security posture. It is also easier to custom configure open-source software, as you can edit the source code to work best for you and your organization including adding more security in the code. Almost all code is not "closed source" as well. Proprietary code can be reverse engineered, so the fact that open-source code is easily available is not a liability to the security of the code. The ability to read the code offers no incentive or opening for attackers compared to closed source code. Another benefit of open-source software is the community. However, one drawback of Open Source Community is the lack of accountability or figure heads. Organizations like to be able to point the finger and blame someone else when things go wrong. Like FireEye being able to say that they were not breached, SolarWinds was breached and it affected FireEye. It is a liability using 0pen-source software for these major organizations because they do not have anyone they can blame to their shareholders if the software is compromised and they are affected.

How secure is open-source software in actuality? Does the risk outweigh the reward? Open-source software is just as secure as proprietary software and even has some benefits compared to proprietary software. These benefits include price, adaptability and responsiveness, and overall community and user group. That is not to say that there are not times and instances where organizations would be better off using proprietary software for reasons shown. Open-source software is just as secure and we saw this by comparing the SolarWinds breach that affected thousands of known secure organizations and the recent Lazurus Open-source software breaches. It is important to remember that no code or software is impenetrable and that the weakest part of any organization's cybersecurity posture is people. No matter how secure the house is, it does nothing if a door is just left open for intruders to access. In conclusion, "open source does not pose any significant barriers to security, but rather reinforces sound security practices by involving many people that expose bugs quickly and offers side-effects that provide customers and the community with concrete examples of reusable, secure, and working code" (3). Open-source software is not any less secure than proprietary software and has great benefits that proprietary software does not have.

Works Cited

[1] Etal. “Check Point Research: Third Quarter of 2022 Reveals Increase in Cyberattacks and Unexpected Developments in Global Trends.” *Check Point Software*, 26 Oct. 2022, https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

[2] “What Is Open source?” *Opensource.com*, https://opensource.com/resources/what-open-source.

[3] Clarke, Russell, et al. “Is Open-source software More Secure?” *CSE P 590TU: Homeland Security / Cyber Security, Autumn 2005*, University of Washington, https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf.

[4] Hoffman, Anton. “Solarwinds Orion Security Breach: A Shift in the Software Supply Chain Paradigm.” *Snyk*, 15 Feb. 2022, https://snyk.io/blog/solarwinds-orion-security-breach-a-shift-in-the-software-supply-chain-paradigm/.

[5] Temple-Raston, Dina. “A 'Worst Nightmare' Cyberattack: The Untold Story of the Solarwinds Hack.” *NPR*, NPR, 16 Apr. 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[6] Goodin, Dan. “Numerous Orgs Hacked after Installing Weaponized Open source Apps.” *Ars Technica*, 29 Sept. 2022, https://arstechnica.com/information-technology/2022/09/north-korean-threat-actors-are-weaponizing-all-kinds-of-open-source-apps/.