Published by Cyber Magazine, 23 July 2017,
http://magazine.milcyber.org/stories/proliferationincybersecurity

Proliferation in Cybersecurity

By Trey Herr

The WannaCry ransomware, and more recent notPetya wiper, are the latest but certainly not the only examples of proliferation when it comes to malicious software. What is this proliferation? Basically – someone writes a piece of malware, a third party finds it, adapts it, adds in some of their own code …et voila, a new piece of malware is born. This latest epidemic is based on a commonly used ransomware, combined with a modified version of the NSA's leaked exploit, and tied together with some new encryption functionality and part of an open source security tool.[1]

Proliferation deals with the diffusion of capabilities, often new weapons technologies, between different actors in the international political system. In cybersecurity, this proliferation describes how groups learn from and reuse tools developed by others, whether intentionally as through collaboration, or unintentionally. Unintentional proliferation is the process whereby the target of a piece of malicious software takes it apart to learn and reuse it. This unintentional proliferation is an issue not unique to cybersecurity but vastly more prominent than in traditional domains of conflict.

Within cybersecurity, intentional proliferation of malware involves direct intelligence support and transfer of software from one party to another. States have no monopoly on capabilities here. Non-state groups are a constant source of innovation on both offense and defense. Proliferation of malware can include a range of different types of information: from highly valuable software vulnerabilities to complete malicious software programs and the supporting infrastructure to covertly deploy them. The skills and capacity of groups on the receiving end of this proliferation can vary dramatically.[2]

If code can move across borders with little more than an email, what does counter-proliferation look like for cybersecurity? Because there are no special weapons materials, like plutonium, necessary to create malware, the challenge becomes how to impose costs on attackers. One answer stems from how many kinds of malware are built. Rather than a weapon like a brick, which can be thrown against nearly any object, most malware depends on a software vulnerability. These vulnerabilities are small flaws

[1] For more on the recent notPetya wiper, see: https://lawfareblog.com/ransomware-remixed-song-remains-same
[2] Portions of this article will appear as a chapter in the upcoming Springer volume, "Cyber Weaponry: Issues and Implications of Digital Arms"

in software which an attacker, or curious researcher, could take advantage of to manipulate the target computer.

By reducing the supply of these software vulnerabilities, defenders can raise attacker's cost to develop and use malicious software. To achieve this, governments should reduce the number and significance of software vulnerabilities (on which malware often depends) by encouraging more effective vulnerability discovery, disclosure, and patching by private companies and researchers. In a new paper, I suggest ten things the policy community in the United States can do to reduce the supply of vulnerabilities and help disrupt the activity of attackers.[3] The goal with any of these policy recommendations isn't to 'solve' a problem – security is not something in need of a solution but rather gradual process improvements. Proliferation in cybersecurity is a low cost activity for attackers right now but policymakers can do more to change that.

About the Author

Trey Herr, Ph.D, is a postdoctoral fellow with the Belfer Center's Cyber Security Project at the Harvard Kennedy School. His work focuses on trends in state developed malicious software, the structure of criminal markets for malware components, and the proliferation of malware. Trey is co-editor of Cyber Insecurity — Navigating the Perils of the Next Information Age, an edited volume on cybersecurity policy, and is a non-resident fellow with New America's Cybersecurity Initiative. He previously worked with the Department of Defense to develop a risk assessment methodology for information security threats. He holds a Ph.D. and M.A. in Political Science from George Washington University and a B.S. in Theatre and Political Science from Northwestern University.

Photo credits: Photo in article from infosecinstitute.com

[3] For more on this, see: *Countering the Proliferation of Malware: Targeting the Vulnerability Life Cycle* - http://www.belfercenter.org/sites/default/files/files/publication/CounteringProliferationofMalware.pdf