COUNCIL *on*
FOREIGN
RELATIONS

CYBER BRIEF

Using Incentives to Shape the Zero-Day Market

Adam Segal

September 2016

This Cyber Brief is part of the Digital and Cyberspace Policy program.

In early 2016, the Federal Bureau of Investigation reportedly paid more than $1.3 million for a software flaw that allowed it to unlock an iPhone without Apple's assistance. The purchase was possible because there is a market for previously unknown vulnerabilities, often referred to as "zero-days" because the vendor has had zero days to patch the vulnerability. Estimates of the size of the market vary widely, but its operation affects the security of individuals, companies, and governments.

When hackers and security researchers find a software flaw—also known as a bug—they can exploit it by creating software or sequencing commands that take advantage of the vulnerability, reveal it publicly, disclose or sell it to the software vendor as part of a bug bounty program, or sell it to a third party such as a criminal network, broker, defense contractor, or government agency. When governments acquire zero-days, they have similar choices: reveal the flaw or choose to keep it secret, building a stockpile for intelligence gathering or offensive operations.

There has been a growing debate over the role the U.S. government could and should play in the zero-day market. Some experts have suggested that the federal government corner the market, purchasing all known zero-days and revealing the vast majority of zero-days that it buys or discovers. Others want to regulate the market and make the sale of zero-days to bad actors illegal. Attempts to either monopolize or restrict the zero-day market to specific actors are, however, likely not only to fail but also to undermine security by handicapping legitimate research.

Instead of overreaching to regulate the entire zero-day market, the U.S. government should create incentives for individuals, companies, and governments to find software vulnerabilities, publicize, and patch them, and thus reduce the risk of attack. The U.S. government should expand exemptions for security research under criminal and copyright law, promote secure software engineering early in a product's development, and expand bug bounty programs throughout the federal system.

BACKGROUND

Although a market for vulnerabilities has existed almost as long as software itself, many early security researchers reported vulnerabilities less for financial reward and more in hope of recognition from other hackers or to make software more secure. As demand for vulnerabilities has increased, software has become more complex, and the pool of individuals with the expertise to conduct security research has grown, economic incentives and bug bounty programs have proliferated. The programs have spread from the tech giants—Adobe, Facebook, Google, and Microsoft—to more conventional sectors of the economy—General Motors and United Airlines—and the U.S. government. Specialized platforms that connect companies wishing to run bug bounty programs have also emerged.

A RAND Corporation report distinguishes vulnerability markets based on the initial buyer (software vendors, governments, criminals) and intended use of the zero-day (defense, defense and offense, offense). The report also differentiates the markets based on when a bug is disclosed to the vendor. In white markets, a vulnerability is immediately sold or given to the vendor. In gray markets, vulnerabilities may eventually make it back to the vendor but after a delay or use by others. In black markets, vulnerabilities never make it back to the software vendor. In all cases, the seller often also provides proof that the discovered vulnerability can be exploited, from a basic proof of concept in the white markets to something fully functional and reliable in the gray and black markets.

In white markets, bug bounty programs have made it easier for buyers and sellers to find one another. Gray markets are smaller and more dependent on personal relationships. In black markets, identifying legitimate buyers and sellers is challenging. Moreover, in gray and black markets, buyers and sellers rarely publicly disclose vulnerability prices, making it difficult to estimate the size and value of those markets. Prices reportedly range from a few thousand dollars to hundreds of thousands of dollars, with a few up to $1 million. Although criminal groups account for some of the demand for offensive uses, some evidence suggests that nation-states are the primary drivers.

CHALLENGES

Although the U.S. national security community has seized on zero-days as an important issue, those conducting offensive cyber operations warn against placing too much emphasis on them. For example, National Security Agency officials have downplayed the significance of zero-days and stressed the importance of an attacker's persistence and focus instead. Most attacks do not rely on zero-days, but instead exploit known vulnerabilities that have not yet been patched.

Regulating the market is difficult because it is problematic to define a zero-day. Policymakers often frame zero-days as distinct commodities and thus susceptible to definition and regulation, but those involved in finding or exploiting zero-days see them as composed of multiple parts: the vulnerability as well as the exploits and techniques that make use of it. For the policymaker, a zero-day looks like a weapon or a defensive tool with a stable set of buyers and sellers and knowable development costs, uses, and lifespan. To vulnerability traders, the zero-day is more like information, always in flux. The lack of market transparency means possessors of a zero-day are uncertain if they discovered it first or whether others know about it. The value of a zero-day may increase as multiple exploits are developed, or it may collapse if the bug is patched, others find and benefit from the zero-day, or the targeted software becomes obsolete.

Even if more pricing information is available, it might reveal little about a bug's importance. Some of the objectives attached to a particular vulnerability, such as political espionage or disruption of a target for political goals, may not have an economic value.

In addition, if software will always have large numbers of vulnerabilities, then it is unlikely that software vendors can keep up with the sums bug buyers are willing to pay. Large payouts may create perverse incentives, drawing a finite pool of security researchers to focus on after-market vulnerability discovery instead of preventing vulnerabilities in code in the first place. The overlap between the bugs the defender knows about and those the attacker is aware of may be small. As a result, a large number of purchases in one market may do little to reduce the threat.

The global nature of the market will also hamper domestic efforts at regulating the sale of zero-days to criminals, terrorists, or potential adversaries. As with other attempts to control dual-use goods, some countries may adopt a laissez-faire attitude. For example, Hacking Team, an Italian company with operations in over forty countries, sells tools that exploit vulnerabilities. Therefore, a domestic policy not matched by a multilateral effort is unlikely to succeed.

Most security research is dual use—offensive knowledge is required for defense and vice versa—so limits on certain types of exploits could have unintended consequences. Attempts to restrict the sale of zero-days may penalize researchers, making computer networks less secure. A recent effort to keep hacking tools out of the wrong hands under the Wassenaar Arrangement, a multilateral agreement on export controls on arms and dual-use technologies, for example, failed to distinguish between offensive software and legitimate network management and security software. After protests from computer security experts, the U.S. government is now revising the effort, but, had the agreement moved forward, it would have handicapped the work of bug hunting, vulnerability patching, and network security testing.

RECOMMENDATIONS

Any attempt to regulate the buying and selling of zero-days is bound to fail. Although there are regulations of other forms of markets where intellectual property is bought and sold, these markets have neither the secrecy that characterizes buyers and sellers nor the mutability of the value, use, and properties of zero-days. Instead, policy should be focused to encourage bug disclosure, where appropriate, and to mitigate known threats.

One method to incentivize disclosures is to expand exemptions for security research under copyright law and the Computer Fraud and Abuse Act (CFAA). In the past, software vendors have used copyright law to threaten security researchers who have publicly disclosed vulnerabilities. To test the security of software, researchers often have to disable copy protection systems, an action prohibited by U.S. copyright law. Although the Library of Congress can grant exemptions, it does so on a case-by-case basis—as it recently did for the hacking of software running in cars, allowing researchers to act without fear of lawsuits from manufacturers—but these exemptions are temporary and take several years to be granted. The exemption process should be streamlined and expanded to other sectors.

The CFAA makes it illegal to intentionally access a computer without authorization or in excess of authorization. The statute, however, does not define what authorization or in excess mean, and the penalties are often disproportionate to the perceived crime. The lack of clarity and the threat of severe punishment can prevent legitimate security research, as finding bugs often requires exceeding authorized access. Useful reform of the act would clarify the definitions of damages caused by computer crimes, and make penalties proportional to damages.

The Defense Advanced Research Projects Agency (DARPA) has done much research on secure software development, a security process that does not rely on finding bugs and issuing patches after they are discovered but rather prevents the introduction of vulnerabilities in the coding stage. The federal government and the private sector should invest more in automation to identify vulnerabilities, but DARPA can also do more to make its tools and techniques usable and widely distributed. For example, DARPA publishes code on its website, but much of it is research prototypes, not usable tools, and researchers cannot tell which code is new and what is being maintained. DARPA should more actively publicize new code, create incentives for researchers to publish code in open source formats, and push out more code on GitHub, a widely used software hosting platform, which would give more visibility to its efforts and more avenues for research.

In April 2016, the Department of Defense announced Hack the Pentagon, a bug bounty program for vulnerabilities in government systems. It involved about 250 hackers finding 138 vulnerabilities in less than a month, with payouts as high as $15,000. All hackers were required to undergo background checks and were limited to public-facing networks, not the Pentagon's most sensitive systems. This program should be expanded across the government. In addition, regulatory agencies could create sanctions for specific sectors to improve their security. The Food and Drug Administration, for example, could penalize medical device companies for failing to live up to their products' security claims by requiring companies to pay into a pool for bug bounty programs to identify security flaws in networked medical devices.

Critics may complain that these policies essentially leave zero-day markets untouched. Even the most successful efforts to reduce the introduction of bugs in software will not eliminate vulnerabilities and will thus leave a zero-day market in place. Zero-days, however, are not like traditional commodities and experience has shown that policymakers are often ill-equipped to translate computer security terminology into clear regulatory text. U.S. policymakers should recognize this and opt for these alternative methods that have broad support in the technical community.

About the Author

Adam Segal is Ira A. Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy program at the Council on Foreign Relations. An expert on security issues, technology development, and Chinese domestic and foreign policy, Segal was the project director for the CFR-sponsored Independent Task Force report *Defending an Open, Global, Secure, and Resilient Internet*. His book *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* describes the increasingly contentious geopolitics of cyberspace. His work has appeared in the *Financial Times*, *Economist*, *Foreign Policy*, *Wall Street Journal*, *Washington Post*, and *Foreign Affairs*, among others. He writes for the blog *Net Politics*.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.

Copyright © 2016 by the Council on Foreign Relations® Inc.
All rights reserved.

This paper may not be reproduced in whole or in part, in any form beyond the reproduction permitted by Sections 107 and 108 of the U.S. Copyright Law Act (17 U.S.C. Sections 107 and 108) and excerpts by reviewers for the public press, without express written permission from the Council on Foreign Relations.