Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

News & Highlights

Hacking Contests Offer Big Payouts for Exposing Security Flaws

Mitch Leslie

Senior Technology Writer

Like any competitor, Yueqi Chen was anxious as he awaited the chance to demonstrate his skill in public. It was the afternoon of 19 May 2022, and Chen, then a visiting fellow in computer science at Northwestern University in Evanston, IL, USA, was sitting at a cloth-draped table in front of a small audience at Pwn2Own 2022 Vancouver, a computer hacking competition held at the Vancouver Sheraton Wall Centre in Canada [1]. This session of the competition would test an exploit—invasive code that takes advantage of a security vulnerability—that Chen and his colleague Zhenpeng Lin, a Northwestern University doctoral student, had devised to seize control of the Ubuntu Desktop, a widely used operating system.

After the event's emcee introduced Chen and explained the challenge, the trial started. A conference staff member sitting next to Chen launched the exploit on a laptop, and a bright digital clock on the corner of the table began counting down from 5 min. Ratcheting up the tension, the previous contestants, who attempted to hack a Tesla car, had failed to get their exploit to work after trying for 1 h, said Chen, and "that made me very nervous." But after only 18 s, the message "UID = 0" popped up on the laptop's screen and the calculator app opened, signaling that Chen and Lin's exploit had provided root access, or administrator-level control [2]. A malicious, or "black hat," hacker with the same privileges could steal or modify data and perform other kinds of mischief. "It is a very impactful exploit," said Chen, now an assistant professor of computer science at the University of Colorado, Boulder, USA.

Pwn2Own 2022 Vancouver awarded more than 1.1 million USD in prizes—Chen and Lin received 40 000 USD for their feat [3]. The sponsor of the contest, an Austin, TX, USA-based organization called the Zero Day Initiative, typically holds two such competitions per year. So-called ethical, or "white hat," hackers who expose vulnerabilities can earn recognition and hefty rewards at other events as well. The most recent edition of China's Tianfu Cup in 2021, for instance, doled out about 1.9 million USD for hacking, among other products, the latest iPhone [4,5].

Many of the companies whose products are compromised have embraced such events as a means to improve security [6]. By inviting scrutiny from many of the world's best ethical hackers, the "victims" can identify and patch flaws before black hat hackers make use of them. Some critics, however, dismiss the value of the contests. They focus on "one-off hacks" and do not provide the systematic analysis of security weaknesses that is necessary to protect against intrusions, said Sujeet Shenoi, professor of computer science at the University of Tulsa, OK, USA. Shenoi has been teaching students the finer points of computer security for more than 20 years.

What computer security experts do agree on is that hacking is a growing and increasingly costly problem (Fig. 1) [7]. "There are attacks all the time, and many times they cannot be detected because they are so good," said Shenoi. Hackers have recently pulled off some destructive and expensive intrusions. In 2022, two ransomware attacks against the government of Costa Rica threw the country's economy and medical system into chaos, forcing some government offices to return to paper forms [8]. The previous year, a separate ransomware attack caused the company Colonial Pipeline to shut down its entire 8800 km system of pipelines, which deliver almost half of the gasoline, diesel, and aviation fuel for the East Coast of the United States [9,10]. In response, gasoline prices jumped, and the US government declared a state of emergency in the affected areas [11]. The company paid almost 5 million USD to a hacker group to unlock its data [9].

It is little consolation to those who suffered the attack, but the hackers who targeted Colonial Pipeline were only after money [11].

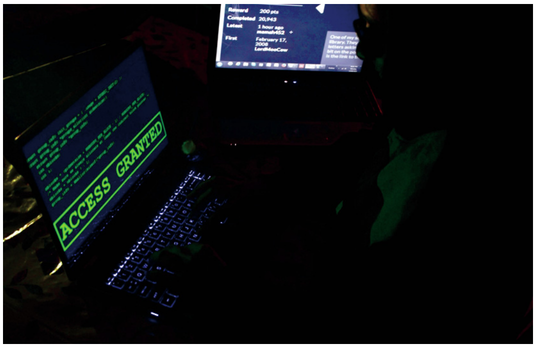

Fig. 1. Each time hackers break into a corporate computer system, the intrusion costs the hacked company an average of 4.4 million USD, according to recent estimates [7]. The potential damage and cost of such violations have made legitimate hacking contests a popular means for digital developers to try to preempt the risk—and an increasingly lucrative activity for contestants. Credit: Public domain (CC0).

https://doi.org/10.1016/j.eng.2022.08.002

They share that motivation with many cyber intruders, said Shenoi. The other threats that keep him and his students up at night come from countries that are pursuing different goals, including stealing secrets and undermining key systems like power grids. Many countries employ skilled corps of hackers. They have also bought powerful hacking tools such as the scandal-ridden Pegasus spyware developed and sold by an Israeli company, which the United States hit with sanctions in 2021 [12,13].

Vulnerabilities that malicious hackers can leverage are always present in software and hardware. "Any system that is complex can be attacked," Shenoi said. Although companies cannot stop all intrusions, they can make these vulnerabilities harder to exploit, said Daan Keuper, head of security research at Computest, a computer security consultancy based in Zoetermeer, the Netherlands. But first somebody must find them.

Contests are not the only mechanism for uncovering security holes. Many companies, organizations, and even the US Department of Defense pay bounties to researchers who report these problems. One bug bounty program whose clients include Google and Netflix awarded nearly 45 million USD in one year, and nine hackers who reported vulnerabilities to the program have earned at least 1 million USD each in less than a decade [14].

Nonetheless, Pwn2Own and similar competitions have become increasingly important for identifying vulnerabilities. Pwn2Own began in 2007 as a challenge during a security conference to hack Apple's latest MacBook Pro, which the company's advertisements claimed were unhackable [15]. The winning duo uncovered a vulnerability in 5 h [15]. "Pwn" is hacker slang for taking control of a machine or system, and they got to keep the MacBook they hacked, hence the name of the contest.

The event has become more lucrative since then. The more than 1.1 million USD doled out at the Vancouver event was the most the Zero Day Initiative has awarded to date. The overall winner, or "Master of Pwn," was a security company from Singapore called STAR Labs, which took home 270 000 USD after breaking into the Ubuntu Desktop, Windows 11, Microsoft Teams, and VirtualBox [16]. One individual hacker not connected to that lab earned 150 000 USD for his exploits [16].

Chen and Lin said the opportunity to win prize money was one reason they entered Pwn2Own. Prestige was another. The contest is "like the Oscars of the hacking community," said Chen. A few weeks before each event, the organizers publish targets, or types of attacks against specific systems that competitors must perform to win. Working with their sponsor Xinyu Xing, an associate professor of computer science at Northwestern University, Chen and Lin discovered how to perform a so-called escalation of privilege attack against the Ubuntu Desktop, which can give an unauthorized user access to data, security settings, and connected systems [2]. Their exploit targets a vulnerability they uncovered by chance in the kernel, a key part of the operating system that allocates memory and performs other crucial tasks [17].

For many companies, Pwn2Own and similar events provide additional security tests for their products. After demonstrating their exploit in a public session, contestants meet with representatives of the vendor whose hardware or software they hacked to reveal the specifics of the attack. The vendor then has 90 days to patch the problem before the Zero Day Initiative publishes the details of the vulnerability [1]. Some hacking victims respond promptly. Mozilla, the non-profit that distributes the Firefox web browser, fixed bugs revealed at Pwn2Own Vancouver 2022 two days after the contest [18].

A benefit of the "bug hunting" approach of competitions like Pwn2Own, say advocates, is that it forces companies to accept that security glitches are inevitable—and to take measures to limit the damage hackers can cause [19]. As one commentary put it, "Pwn2Own is the perfect antidote to fanboys who say their platform is safe" [19].

The contests can also shine a spotlight on whole industries that need to clean up their act. Pwn2Own's event in April 2022 in Miami, FL, USA, for example, exposed worrying flaws in industrial control systems (ICS), which manage facilities such as power plants, pipelines, and factories [20]. Keuper and his hacking partner Thijs Alkemade, also a security researcher at Computest, earned the "Masters of Pwn" crown and 90 000 USD for exploiting four kinds of ICS software, including the widely used Open Platform Communications United Architecture (OPC UA) protocol that allows data sharing [20]. The most disturbing aspect of the competition was how easy the targets were to penetrate. When it comes to security, "ICS applications are a number of years behind normal information technology applications," said Alkemade.

However, competitions like Pwn2Own have also drawn criticism. Skeptics complain that instead of increasing security, the format makes it easier for unscrupulous hackers to identify vulnerabilities and sell them to criminals or hostile countries—who would pay more than the contests [21]. In addition, because of cost or other obstacles, there is no guarantee that companies will address the flaws revealed at the competitions. A company may be reluctant to fix an ICS vulnerability, for instance, because it would require shutting down production at its factory [6].

The large number of security lapses contestants find—and the amount of money companies are willing to pay out in bug bounties for software and hardware that is already on the market—also raise the question of why the products are not made safer before release. Keuper said he is skeptical that public exposure through contests like Pwn2Own will spur vendors to be more careful. "There is no money to be made cleaning up software. Companies want to push new features," he said.

Shenoi and his students—he has trained more than 400 of them—take a different approach to improving security. To identify vulnerabilities, they have hacked a wide range of systems, including US voting machines, the Norwegian power grid, pacemakers, wind farms, and several models of rental cars. However, they do not reveal their results at contests, and they do not accept money for their work, he said. And instead of pinpointing individual flaws, they perform more comprehensive security assessments. "We want to understand the whole network, all the ways to hit a target," he said.

Despite these misgivings, contests like Pwn2Own will continue. And Chen and Lin say they are already preparing. "We know of other vulnerabilities in the Ubuntu Desktop kernel, so we will go next year," said Lin.

References

[1] Childs D. Pwn2Own 2022 Vancouver: the results [Internet]. Irving: Zero Day Initiative; 2022 May 18 [cited 2022 Jul 1]. Available from: https://www.zerodayinitiative.com/blog/2022/5/18/pwn2own-vancouver-2022-the-results.

[2] Understanding privilege escalation and 5 common attack techniques [Internet]. Boston: Cynet; c2022 [cited 2022 Jul 1]. Available from: https://www.cynet.com/network-attacks/privilege-escalation/.

[3] Haworth J. Pwn2Own Vancouver: 15th annual hacking event pays out $1.2 m for high-impact security bugs [Internet]. Knutsford: The Daily Swig; 2022 May 23 [cited 2022 Jul 1]. Available from: https://portswigger.net/daily-swig/pwn2own-vancouver-15th-annual-hacking-event-pays-out-1-2m-for-high-impact-security-bugs.

[4] Winder D. iPhone pro hacked: Chinese hackers suddenly break iOS 15.0.2 security [Internet]. New York City: Forbes; 2021 Oct 18 [cited 2022 Jul 1]. Available from: https://www.forbes.com/sites/daveywinder/2021/10/18/iphone-13-pro-hacked-chinese-hackers-suddenly-break-ios-1502-security.

[5] Kovacs E. $1.9 m paid out for exploits at China's Tianfu Cup Hacking Contest [Internet]. Boston: Security Week; 2021 Oct 19 [cited 2022 Jul 1]. Available from: https://www.securityweek.com/19-million-paid-out-exploits-chinas-tianfu-cup-hacking-contest.

[6] Greenberg A. Inside the world's highest-stakes industrial hacking contest [Internet]. San Francisco: Wired; 2020 Jan 23 [cited 2022 Jul 1]. Available from: https://www.wired.com/story/pwn2own-industrial-hacking-contest/.

[7] Rivero N. Why the cost of getting hacked is higher than ever [Internet]. New York City: Quartz; 2021 Jul 28 [cited 2022 Jul 14]. Available from: https://qz.com/2039599/why-the-cost-of-getting-hacked-is-higher-than-ever/.

[8] Burgess M. Conti's attack against Costa Rica sparks a new ransomware era [Internet]. San Francisco: Wired; 2022 Jun 12 [cited 2022 Jul 11]. Available from: https://www.wired.com/story/costa-rica-ransomware-conti/.

[9] Wilkie C. Colonial pipeline paid $5 million ransom one day after cyberattack, CEO tells senate [Internet]. New York City: CNBS; 2021 Jun 8 [cited 2022 Jul 1]. Available from: https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

[10] Morrison S. How a major oil pipeline got held for ransom [Internet]. New York City: Vox; 2021 Jun 8 [cited 2022 Jul 1]. Available from: https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

[11] Russon MA. US fuel pipeline hackers "Didn't mean to create problems" [Internet]. London: BBC News; 2021 May 10 [cited 2022 Jul 1]. Available from: https://www.bbc.com/news/business-57050690.

[12] Farrow R. How democracies spy on their citizens [Internet]. New York City: New Yorker; 2022 Apr 18 [cited 2022 Jul 1]. Available from: https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

[13] Mazzetti M, Bergman R. Defense firm said US spies backed its bid for pegasus spyware maker [Internet]. New York City: New York Times; 2022 Jul 11 [cited 2022 Jul 11]. Available from: https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html.

[14] Ranger S. Cybersecurity: this is how much top hackers are earning from bug bounties [Internet]. New York City: ZDNet; 2020 Sep 22 [cited 2022 Jul 14]. Available from: https://www.zdnet.com/article/this-is-how-much-top-hackers-are-earning-from-bug-bounties/.

[15] Fiscutean A. How Pwn2Own made bug hunting a real sport [Internet]. London: Dark Reading; 2022 May 19 [cited 2022 Jul 1]. Available from: https://www.darkreading.com/edge-articles/how-pwn2own-made-bug-hunting-a-real-sport.

[16] Ziemann F. Microsoft teams and Windows 11 hacked multiple times [Internet]. Dover: NewsABC; [cited 2022 Jul 1]. Available from: https://newsabc.net/microsoft-teams-and-windows-11-hacked-multiple-times/.

[17] Chin M. How a university got itself banned from the Linux kernel [Internet]. New York City: The Verge; 2021 Apr 30 [cited 2022 Jul 1]. Available from: https://www.theverge.com/2021/4/30/22410164/linux-kernel-university-of-minnesota-banned-open-source.

[18] Brown E. Mozilla releases fixes for Firefox, Thunderbird vulnerabilities exploited during Pwn2Own Vancouver 2022 Hacking Contest [Internet]. New York City: iTech Post; 2022 May 25 [cited 2022 Jul 1]. Available from: https://www.itechpost.com/articles/110888/20220525/mozilla-releases-fixes-firefox-thunderbird-vulnerabilities-exploited-during-pwn2own-vancouver.htm.

[19] Goodin D. Pwn2Own is the perfect antidote to fanboys who say their platform is safe [Internet]. New York City: Ars Technica; 2014 Mar 14 [cited 2022 Jul 1]. Available from: https://arstechnica.com/information-technology/2014/03/pwn2own-the-perfect-antidote-to-fanboys-who-say-their-platform-is-safe/.

[20] O'Neill PH. These hackers just showed how easy it is to target critical infrastructure [Internet]. Cambridge: MIT Technology Review; 2022 Apr 21 [cited 2022 Jul 1]. Available from: https://www.technologyreview.com/2022/04/21/1050815/hackers-target-critical-infrastructure-pwn2own/.

[21] Keizer G. Three-time Pwn2Own winner knocks hacking contest rules [Internet]. Needham: Computerworld; 2011 Feb 28 [cited 2022 Jul 1]. Available from: https://www.computerworld.com/article/2506261/three-time-pwn2own-winner-knocks-hacking-contest-rules.html.