Contents lists available at ScienceDirect

Engineering

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

News & Highlights

黑客大赛为发现安全漏洞者提供巨额奖金

Mitch Leslie

Senior Technology Write

和其他参赛者一样，Yueqi Chen焦虑地等待着在公众面前一展身手的机会。那是2022年5月19日的下午，当时正在美国伊利诺伊州埃文斯顿西北大学作计算机科学访问学者的Chen正坐在Pwn2Own 2022温哥华黑客大赛现场的一张铺着布的桌子前，面前是为数不多的观众，本次大赛在加拿大温哥华喜来登华尔中心酒店举行[1]。本场比赛将测试一个由Chen和他的同事、西北大学博士生Zhenpeng Lin共同设计的针对广泛使用的Ubuntu操作系统安全漏洞的攻击代码。

在主持人介绍完Yueqi Chen并解释了大赛任务后，比赛就开始了。坐在Chen旁边的一名会议工作人员在笔记本电脑上启动了漏洞利用，桌子角落上一个明亮的数字时钟从5分钟开始倒计时。Chen说，前面几位试图非法入侵特斯拉汽车的参赛者在尝试了1小时后仍未能成功，“这让我非常紧张。”但仅仅过了18秒，笔记本电脑屏幕上弹出消息“UID = 0”，计算器应用程序打开，表示Chen和Lin的漏洞利用程序获得了超级管理员访问权限或管理员级控制权限[2]。此时，具有相同权限的恶意黑客或“黑帽”黑客便能够窃取或修改数据并进行其他类型的破坏。“这是一个非常成功的漏洞利用程序，”现为美国科罗拉多大学博尔德分校计算机科学助理教授的Chen说。

Pwn2Own 2022温哥华黑客大赛颁发的奖金超过110万美元，Chen和Lin因出色的表现获得了4万美元的奖金[3]。大赛的赞助商是美国得克萨斯州奥斯汀市一个名为“零日计划”（Zero Day Initiative）的组织，通常每年举办两次。专注于排查安全漏洞的所谓道德黑客或“白帽”黑客也可以在其他赛事中获得认可和丰厚的奖金。例如，2021年中国“天府杯”国际网络安全大赛总奖金额达到约190万美元，其中包括一个破解最新款iPhone手机的比赛项目[4–5]。

产品遭到入侵的许多公司都将此类活动作为提高安全性的一种手段[6]。通过邀请世界上众多最优秀的道德黑客进行审查，“受害者”可以在“黑帽”黑客利用漏洞之前识别并修补这些漏洞。然而，一些评论家认为这类比赛的价值不大。美国俄克拉何马州塔尔萨大学计算机科学教授Sujeet Shenoi表示，这些比赛只关注“一次性黑客攻击”，而不对安全漏洞进行系统分析以防范非法入侵。20多年来，Shenoi一直在从事计算机安全的教学工作。

计算机安全专家一致认为，黑客攻击是一个越来越严重、付出代价越来越高的问题（图1）[7]。Shenoi说：“黑客攻击一直存在，但很多时候无法检测到，因为他们手段高明。”黑客最近发起了一些破坏性的、代价高昂的入侵。2022年，两起针对哥斯达黎加政府的勒索软件攻击事件使该国经济和医疗系统陷入混乱，迫使一些政府部门重新使用纸质表格办公[8]。2021年，另外一起勒索软件攻击事件导致Colonial Pipeline公司关闭了其整个8800 km长的管道系统，这些管道为美国东海岸输送了近一半的汽油、柴油和航空燃料[9–10]。事件导致的后果是汽油价格飙升，美国政府宣布受影响地区进入紧急状态[11]。该公司向一个黑客组织支付了近500万美元后才解

英文原文：Engineering 2022, 17(10): 10–12
引用本文：Mitch Leslie. Hacking Contests Offer Big Payouts for Exposing Security Flaws. *Engineering*, https://doi.org/10.1016/j.eng.2022.08.002

锁了数据[9]。

事实上，攻击Colonial Pipeline的黑客只为谋财，虽然这对于被攻击方算不上是什么安慰[11]。Shenoi说，许多网络入侵者都是为了谋财。让他和学生们夜不能寐的其他威胁来自于一些追求不同目标的国家，包括窃取机密和破坏电网等关键系统。许多国家雇佣了技术熟练的黑客队伍，还购买了强大的黑客工具，如丑闻缠身的间谍软件Pegasus。该软件由以色列一家公司开发并出售，美国于2021年对其进行了制裁[12–13]。

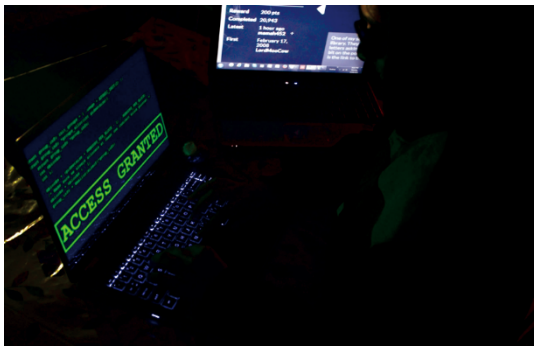

图1. 据最新的估计，黑客每次入侵公司计算机系统，遭受入侵的公司平均损失440万美元[7]。此类违法行为的潜在损失和费用使得合法的黑客大赛成为数字开发人员试图先发制人的一种手段，也使得参赛者获利越来越多。来源：公共领域（CC0）。

恶意黑客可以利用的漏洞总是存在于软件和硬件中。Shenoi说："任何复杂的系统都可能受到攻击。"总部位于荷兰祖特尔梅尔的计算机安全咨询公司Computest的安全研究主管Daan Keuper表示，尽管公司无法阻止所有入侵，但他们可以让这些漏洞难以被黑客利用。但前提是他们必须能够提前找到这些漏洞。

比赛并不是发现安全漏洞的唯一途径。许多公司、组织，甚至美国国防部都向报告这些问题的研究人员支付酬金。客户包括谷歌和Netflix的一个漏洞奖励计划在一年内发出的奖励近4500万美元，九名向该计划报告漏洞的黑客在不到十年的时间里每人至少赚了100万美元[14]。

尽管如此，Pwn2Own和类似的比赛对于识别漏洞变得越来越重要。2007年，在一次安全会议上，Pwn2Own作为一项挑战赛首次亮相，挑战内容是入侵苹果公司最新款MacBook Pro——苹果公司的广告称黑客无法侵入该电脑[15]。获胜的二人组在5小时内发现了一个漏洞[15]。"Pwn"是黑客俚语，意思是入侵或控制机器或系统；大赛获胜者可以获得（Own）被他们攻破的MacBook电脑（作为奖励）——大赛的名字（Pwn2Own）由此而来。

从那时起，这项活动变得更加有利可图。在温哥华这届大赛上发放的110多万美元是"零日计划"迄今为止发放的最高金额。本届总冠军，即"Pwn大师"，是新加坡的一个名为STAR Labs的安全公司，在侵入Ubuntu桌面系统、Windows 11、Microsoft Teams和VirtualBox之后，该公司获得了27万美元奖励[16]。一名与该实验室无关的黑客因其漏洞利用的成果而赚取了15万美元[16]。

Chen和Lin表示，他们参加Pwn2Own大赛的一个目的是赢取奖金，另一个目的是赢得声望。Chen说，这场比赛"就好比黑客界的奥斯卡奖"。在每场比赛前几周，组办方会公布针对特定系统的攻击目标或类型，参赛者必须完成这些攻击才能获胜。Chen和Lin与他们的资助人、西北大学计算机科学副教授Xinyu Xing合作，发现了对Ubuntu桌面系统进行所谓的权限提升攻击的方法，从而允许未经授权的用户访问数据、修改安全设置和访问联网的系统[2]。他们攻击的目标是一个在内核中偶然发现的漏洞，内核是操作系统的一个关键部分，用于分配内存和执行其他关键任务[17]。

对于许多公司来说，Pwn2Own大赛和类似活动为他们的产品提供了额外的安全测试。在公开展示了他们的漏洞利用程序后，参赛者与硬件或软件遭受入侵的供应商代表会面，揭露黑客攻击的细节。然后，供应商有90天的时间来修补漏洞，然后由"零日计划"发布漏洞的详细信息[1]。一些遭受黑客入侵的厂商反应迅速。发行火狐浏览器的非盈利组织Mozilla，在Pwn2Own 2022温哥华黑客大赛结束两天后就修复了被发现的漏洞[18]。

支持者表示，像Pwn2Own这种比赛的"漏洞搜索"方法所带来的好处是，它迫使公司接受安全漏洞是不可避免的，并促使它们采取补救措施来限制黑客攻击可能造成的损失[19]。正如一篇评论所说，"对于那些认为自己所用平台是安全的技术迷来说，Pwn2Own是完美的清醒剂。"[19]

这些比赛也可以聚焦需要整顿自身行为的所有行业。例如，2022年4月在美国佛罗里达州迈阿密举办的Pwn2Own赛事揭露了工业控制系统中令人担忧的缺陷，因为工业控制系统管理着发电站、管道和工厂等设施[20]。Keuper和他的黑客合作伙伴Thijs Alkemade（也是Computest的安全研究员），因发现了四种工业控制系统软件的漏洞，包括广泛使用且允许数据共享的OPC UA（开放平台通信统一架构）协议，赢得了"Pwn大师"桂冠和9万美元奖金[20]。竞赛中最令人不安的是目标入侵太容易。谈到安全性，Alkemade说，"工业控制系统应用程序比正常的信息技术应用程序落后很多年。"

然而，像Pwn2Own这样的比赛也受到了批评。怀疑者抱怨说，这种方式不但没有提高安全性，反而使一些毫

无道德原则的黑客更加乐于寻找安全漏洞并将它们卖给犯罪分子或敌对国家，以获取比大赛奖金更高的酬金[21]。此外，出于成本或其他考虑，一些公司可能并不会解决在比赛中揭露的漏洞。例如，一家公司可能不会愿意为了修复工业控制系统漏洞而让工厂停工停产[6]。

参赛者发现的大量安全漏洞，以及公司愿意为已上市软件和硬件支付的漏洞发现奖金，引发了一个问题，即为什么不让产品更安全之后再发布。Keuper 说，通过 Pwn2Own 这样的比赛公开曝光可能会促使供应商更加谨慎。“清理软件漏洞是不赚钱的。公司需要推出新功能。”他说。

Shenoi 和他的 400 多名学生采取了不同的方法来提高安全性。为了识别漏洞，他们对大量系统实施了入侵，包括美国投票机、挪威电网、心脏起搏器、风电场和几个型号的租赁汽车。然而，他们并没有在比赛中公布这些结果，也不接受工作报酬。他们不是为了查明个别漏洞，而是进行更全面的安全评估。他说：“我们想了解整个网络，了解攻击目标的所有方法。”

尽管存在这些疑虑，但像 Pwn2Own 这样的比赛仍将继续。Chen 和 Lin 说他们已经在准备了。Lin 说：“我们知道 Ubuntu 桌面系统内核中还有其他漏洞，所以我们明年还会去参赛。”

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-highimpact-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-chinastianfu-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-ceotestifies-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-theircitizens.

[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-tophackers-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-realsport.

[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-ofminnesota-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-releasesfixes-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/threetime-pwn2own-winner-knocks-hacking-contest-rules.html.