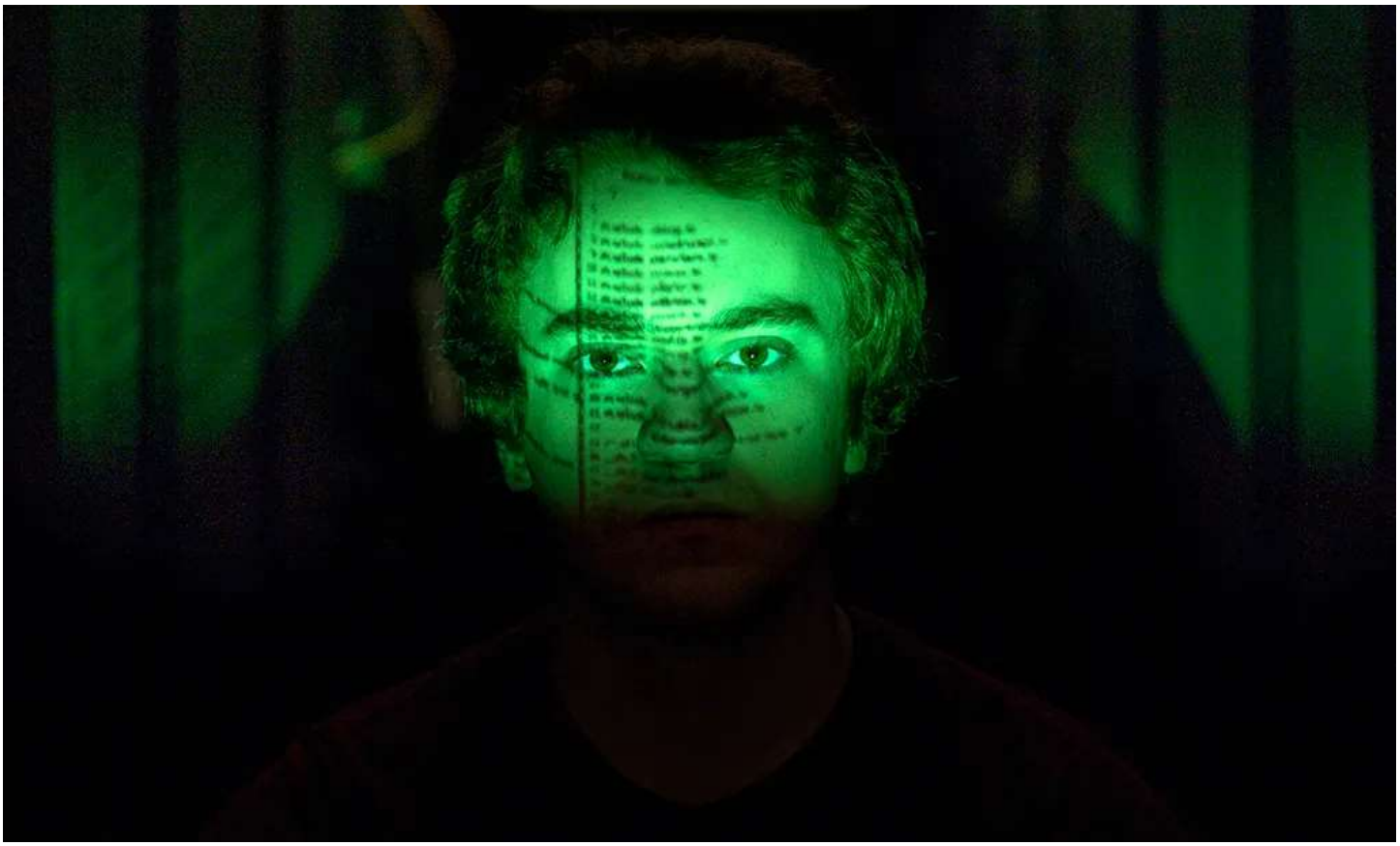
ANDY GREENBERG SECURITY JUL 15, 2014 6:30 AM

Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers

Today Google plans to publicly reveal the team, known as Project Zero, a group of top Google security researchers who will be given the sole mission of finding and neutering the most insidious security flaws in the world's software.



Hacking wunderkind George Hotz's latest gig: An intern on Google's elite hacking team. TRIBUNE REVIEW, ANDREW RUSSELL/AP

WHEN 17-YEAR-OLD GEORGE Hotz became the world's first hacker to crack AT&T's lock on the iPhone in 2007, the companies officially ignored him while scrambling to fix the bugs his work exposed. When he later reverse engineered the Playstation 3, Sony sued him and settled only after he agreed to never hack another Sony product.

When Hotz dismantled the defenses of Google's Chrome operating system earlier this year, by contrast, the company paid him a $150,000 reward for helping fix the flaws he'd uncovered. Two months later Chris Evans, a Google security engineer, followed up by email with an offer: How would Hotz like to join an elite team of full-time hackers paid to hunt security vulnerabilities in every popular piece of software that touches the internet?

Today Google plans to publicly reveal that team, known as Project Zero, a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software. Those secret hackable bugs, known in the security industry as "zero-day" vulnerabilities, are exploited by criminals, state-sponsored hackers and intelligence agencies in their spying operations. By tasking its researchers to drag them into the light, Google hopes to get those spy-friendly flaws fixed. And Project Zero's hackers won't be exposing bugs only in Google's products. They'll be given free rein to attack any software whose zero-days can be dug up and demonstrated with the aim of pressuring other companies to better protect Google's users.

Google security engineer Chris Evans, who is recruiting top talent for Project Zero . ARIEL ZAMBELICH/WIRED

"People deserve to use the internet without fear that vulnerabilities out there can ruin their privacy with a single website visit," says Evans, a British-born researcher who formerly led Google's Chrome security team and will now helm Project Zero. (His business cards read "Troublemaker.") "We're going to try to focus on the supply of these high value vulnerabilities and eliminate them."

Project Zero has already recruited the seeds of a hacker dream team from within Google: New Zealander Ben Hawkes has been credited with discovering dozens of bugs in software like Adobe Flash and Microsoft Office apps in 2013 alone. Tavis Ormandy, an English researcher who has a reputation as one of the industry's most prolific bug hunters most recently focused on showing how antivirus software can include zero-day flaws that actually make users less secure. American hacker prodigy George Hotz, who hacked

Google's Chrome OS defenses to win its Pwnium hacking competition last March, will be the team's intern. And Switzerland-based Brit Ian Beer created an air of mystery around Google's secret security group in recent months when he was credited under the "Project Zero" name for six bug finds in Apple's iOS, OSX and Safari.

Evans says the team is still hiring. It will soon have more than ten full-time researchers under his management; Most will be based out of an office in its Mountain View headquarters, using flaw-hunting tools that range from pure hacker intuition to automated software that throws random data at target software for hours on end to find which files cause potentially dangerous crashes.

Google Vs. The Spooks

And what does Google get out of paying top-notch salaries to fix flaws in other companies' code? Evans insists Project Zero is "primarily altruistic." But the initiative--which offers an enticing level of freedom to work on hard security problems with few restrictions--may also serve as a recruiting tool that brings top talent into Google's fold, where they may later move on to other teams. And as with other Google projects, the company also argues that what benefits the internet benefits Google: Safe, happy users click on more ads. "If we increase user confidence in the internet in general, then in a hard-to-measure and indirect way, that helps Google too," Evans says.

This fits with a larger trend in Mountain View; Google's counter-surveillance measures have intensified in the wake of Edward Snowden's spying revelations. When the leaks revealed that the NSA was spying on Google user information as it moved between the company's data centers, Google rushed to encrypt those links. More recently, it revealed its work on a Chrome plug-in that would encrypt users' email, and launched a campaign to name which email providers do and don't allow for default encryption when receiving messages from Gmail users.

When a zero-day vulnerability gives spies the power to completely control target users' computers, however, no encryption can protect them. Intelligence agency customers pay private zero-day brokers hundreds of thousands of dollars for certain exploits with that sort of stealthy intrusion in mind. And the White House, even as it has called for NSA reform, has sanctioned the agency's use of zero-day exploits for some surveillance applications.

All of that makes Project Zero the logical next step in Google's anti-spying efforts, says Chris Soghoian, a privacy-focused technologist at the ACLU who has closely followed the zero-day vulnerability issue. He points to the now-famous "fuck these guys" blog post by a Google security engineer addressing the NSA's spying practices. "Google's security team is angry about surveillance," Soghoian says, "and they're trying to do something about it."

Like other companies, Google has for years paid "bug bounties"--rewards for friendly hackers who tell the company about flaws in its code. But hunting vulnerabilities in its own software hasn't been enough: The security of Google programs like its Chrome browser often depend on third-party code like Adobe's Flash or elements of the underlying Windows, Mac, or Linux operating systems. In March, Evans compiled and tweeted a spreadsheet, for instance, of all eighteen Flash bugs that have been exploited by hackers over the last four years. Their targets included Syrian citizens, human rights activists, and the defense and aerospace industry.

Colliding Bugs

The idea behind Project Zero, according to former Google security researcher Morgan Marquis-Boire, can be traced back to a late-night meeting he had with Evans in a bar in Zurich's Niederdorf neighborhood in 2010. Around 4am, the conversation turned to the problem of software outside of Google's control whose bugs endanger Google's users. "It's a major source of frustration for people writing a secure product to depend on third party code," says Marquis-Boire. "Motivated attackers go for the weakest spot. It's all well and good to ride a motorcycle in a helmet, but it won't protect you if you're wearing a kimono."

Hence Project Zero's ambition to apply Google's brains to scour other companies' products. When Project Zero's hacker-hunters find a bug, they say they'll alert the company responsible for a fix and give it between 60 and 90 days to issue a patch before publicly revealing the flaw on the Google Project Zero blog. In cases where the bug is being actively exploited by hackers, Google says it will move much faster, pressuring the vulnerable software's creator to fix the problem or find a workaround in as little as seven days. "It's not acceptable to put people at risk by taking too long or not fixing bugs indefinitely," says Evans.

Project Zero bug hunter Ben Hawkes. ARIEL ZAMBELICH/WIRED

Whether Project Zero can actually eradicate bugs in such a wide collection of programs remains an open question. But to make a serious impact, the group doesn't need to find and squash all zero-days, says Project Zero hacker Ben Hawkes. Instead, it only needs to kill bugs faster than they're created in new code. And Project Zero will choose its targets strategically to maximize so-called "bug collisions," the cases in which a bug it finds is the same as one being secretly exploited by spies.

In fact, modern hacker exploits often chain together a series of hackable flaws to defeat a computer's defenses. Kill one of those bugs and the entire exploit fails. That means Project Zero may be able to nix entire collections of exploits by finding and patching flaws in a small part of an operating system, like the "sandbox" that's meant to limit an application's access to the rest of the computer. "On certain attack surfaces, we're optimistic we can fix the bugs faster than they're being introduced," Hawkes says. "If you funnel your research into these limited areas, you increase the chances of bug collisions."

More than ever, in other words, every bug discovery could deny attackers an intrusion tool. "I'm confident we can step on some toes," Hawkes says.

Case in point: When George Hotz revealed his Chrome OS exploit in Google's hacking competition last March to win the contest's six-figure prize, another competition's contestants had simultaneously come up with the same hack. Evans says he also learned of two other private research efforts that had independently found the same flaw---a four-way bug collision. Instances like that are a hopeful sign that the number of undiscovered zero-day vulnerabilities may be shrinking, and that a team like Project Zero can starve spies of the bugs their intrusions require.

"We're really going to make a dent in this problem," Evans says. "Now is a very good time to make a bet on putting a stop to zero-days."

Andy Greenberg is a senior writer for WIRED, covering security, privacy, and information freedom. He's the author of the book *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. The book and excerpts from it published in WIRED won a Gerald Loeb Award for... Read more

SENIOR WRITER