At hacker summit, a new focus on preventing brazen attacks

July 26 2017, by Matt O'brien

In this photo taken Friday, June 8, 2012 Alex Stamos CTO of Artemis Internet, an NCC Group Company, poses by a domain name poster at their offices in San Francisco. Some 2,000 proposals have been submitted as part of the largest expansion of the Internet address system since its creation in the 1980s. These suffixes would rival ".com" and about 250 others now in use. The organization behind it, the Internet Corporation for Assigned Names and Numbers, will announce a full list and other details in London on Wednesday, July 26, 2017. (AP Photo/Eric Risberg, File)

Against a backdrop of cyberattacks that have grown into full-fledged sabotage, Facebook chief security officer Alex Stamos brought a sobering message Wednesday to hackers and security experts at the Black Hat conference.

In short: it's time for hackers once known for relatively harmless mischief to shoulder responsibility for helping detect and prevent major attacks that threaten billions of internet users around the world.

The Black Hat security gathering, happening this week in Las Vegas, follows a series of attacks and data breaches that have paralyzed hospitals, disrupted commerce, caused blackouts and interfered with national elections.

Stamos joined Facebook from Yahoo, which last year disclosed breaches of more than a billion user accounts .

"People now know how important it is to build secure systems to underlie our civilization," Stamos said at a keynote speech. "A topic that was once considered fringe, a topic that we had to fight for respect for, is now on the front page of every newspaper pretty much once a week."

Stamos called for a culture change among hackers and more emphasis on defense—and basic digital hygiene—over the thrilling hunt for undiscovered vulnerabilities. And he called for diversifying an industry that skews white and male, and generally showing more empathy for the people whom security professionals are tasked to protect.

"It's unfair for us to say that users should be better," said Stamos, challenging his profession to find better ways to help people solve the most common vulnerabilities, such as reuse of passwords , email phishing attempts , and not updating devices to patch bugs.

Black Hat has matured since what Stamos, a longtime attendee of the computer security conference, described as its "edgy and transgressive" early days. It has grown more professional and corporate over time. But many of the "really sexy, difficult problems" that security researchers dwell on are far more complicated than the problems that usually harm the average user, he said.

The Nevada event is known for its spectacular demonstrations, such as a hack to spit cash out of an ATM or take remote control of an internet-connected car. Part of that is because of the healthy intellectual curiosity of hackers, but it's also driven by marketing and economic incentives, Stamos said.

"I appreciate the showmanship, but we need a little more thoughtfulness, a little less showmanship in our field," Stamos told reporters after his speech.

Stamos isn't the only one calling for a broader focus on defensive techniques.

"We should celebrate defense," said conference attendee Amit Yoran, CEO of Columbia, Maryland-based security firm Tenable, and a former cybersecurity official during the administration of President George W. Bush. "We focus on the threat of the day, the attack of the day, instead of focusing on the foundational issues."

But some attendees—Stamos among them—also point out that the bug-squashing hacker ethos still plays an important foundational role in helping to understand what needs to be fixed.

"Every single hacker is going to start by attacking and trying to hack things," said Jaime Blasco, a chief scientist at San Mateo, California-based Alienvault, who has been trying to compromise systems since he