UC SANTA BARBARA

THE Current

May 9, 2019

Harrison Tasoff

Mount the Defenses

For the folks on the front lines of network security at UC Santa Barbara, April was a relatively slow month. On an average day, they saw 148,000 attempted cyber-attacks. The average for the previous year? Approximately 280,000 attacks per day.

UC Santa Barbara's network hosts interactions among tens of thousands of people every day. In April, that meant 328 terabytes of traffic moved between the campus and the outside world.

Operating a system of this scale comes with challenges that don't crop up on an average home network. The sheer number of people and devices on a network such as that of the university are sufficient to attract the attention of cyber criminals.

Astounding though they seem, these numbers are probably within normal range for an institution of our size, noted Sam Horowitz, the campus's chief information security officer. And despite it all, activity hums along thanks to the security measures and tireless work of the campus security team.

So how do they do it?

The nature of an attack depends on the goals of the individual behind it. Many incidents are merely attempts to scan the network. "What the scan does is it tries to determine what kind of devices are on the campus, and what kinds of vulnerabilities may exist on those devices," Horowitz explained.

Scans help attackers find out what information is contained on a particular device and whether it’s worth trying to steal. After a scan, an attacker can send malware targeted to a specific vulnerability that was uncovered. This is the most common type of attack. Other attacks attempt to compromise the network or devices on it with malware in order to steal data or recruit the device into serving the attacker. Spyware and viruses are the next most-common types of attack.

Fortunately, the university employs a robust universal threat management system (UTM) to protect the network and its users from them all. The UTM combines the benefits of a firewall with other security measures. This system has helped the campus block over 107 million “incidences of badness,” as Horowitz terms them, since it was installed in December 2017.

Fundamentally, a firewall blocks network traffic based on its characteristics. A simple one uses simple criteria, like the “from” address, the “to” address and the port that traffic is using. Comparing a device’s IP address to a street address, the ports are akin to office or apartment numbers, explained Horowitz. “The port number deals with how the server is listening,” he said. “The server is occupying that office suite and listening for something to come knock on the door.”

The firewall protecting the campus’s network also considers features like a program’s protocol (the most familiar is probably http, or hypertext transfer protocol), its identifying features and its behavior. “And behavior is how you detect scans,” said Horowitz. If the system notices a program bombarding one device with inquiries and then moving on to another device, the UTM will step in and block the scan. The UTM does not, however, look at the actual content of data zipping across the network, Horowitz said.

The firewall also blocks traffic through ports associated with security vulnerabilities, for instance the Microsoft filesharing port. This is why you can’t transfer files through Microsoft file-share between a device off campus and on campus.

The campus security team also takes advantage of layered defenses, much like the different filters in a water purifier: The combination ensures that no bad stuff comes through. These layers include local antivirus software and data encryption, as well as managing who has access to different parts of the network.

Members of the campus community also play a role in this defense. Usernames and passwords factor into network security, as does each individual’s commitment to

keeping devices updated. “You should take the update every time,” said Horowitz. Even behind a firewall, up-to-date software provides yet another layer of defense, closing any vulnerabilities a device may have.

Horowitz also recommends switching off unneeded or unused functions. For example, turn off a device’s ability to host files if you don’t use file-sharing — this decreases its exposure to the frontline. “If you don’t have a service on, you’re not listening for traffic,” he said. So if an attacker targets that channel, “there’s nothing listening. It’s as though they’re talking to an empty room.”

The information security team knows that no defense works 100% of the time. So they also look for issues that may have slipped through the UTM in order to fix the problems they’ve created and strengthen the university’s defenses. Security experts also communicate with each other, driving the evolution of defensive measures in the dynamic landscape of computer security.

“Good security involves both people and technology,” Horowitz said. “We rely on our community to protect their passwords and avoid clicking on phishing links. We use technology to identify and block reconnaissance and attacks that may come our way. Together, these approaches provide a safer environment for the campus to fulfill its mission.”

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.