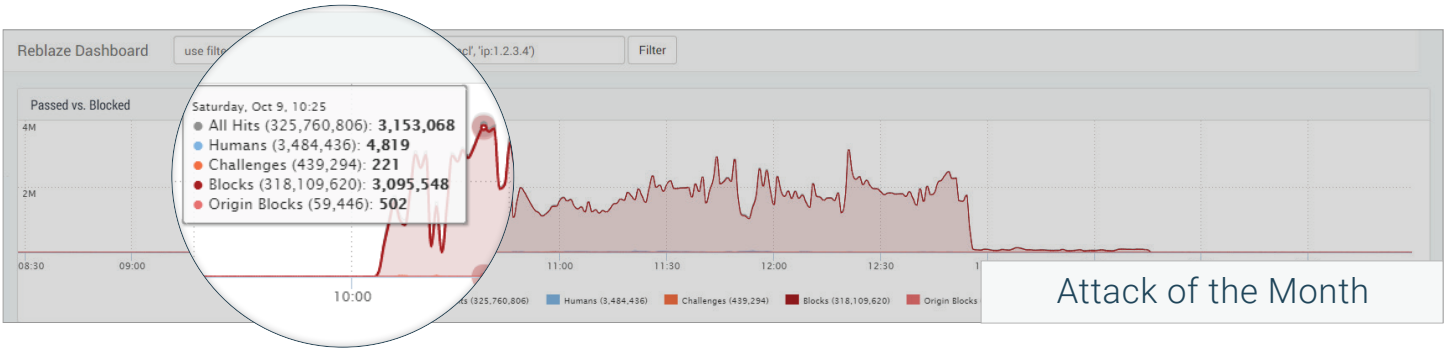

Account Takeover Attack Illustrates a Growing Trend

December 2021: Direct human participation in cyberattacks

Cybercrime has become an extremely lucrative industry. The large hacker groups are making millions of dollars per year. (According to the US Treasury, ransomware payments alone totaled **$590 million** in the first half of 2021.)

This has created two growing trends: first, a rising complexity of threats, because the hackers are hiring top programming talent. (Some advertise openly on job boards in Russia and other CIS countries.) Second, more human participation in cyberattacks, because they are also building teams of skilled operators for their attack tools.

Most attacks are still automated. However, we are observing a growing number of incidents where humans are directly involved, systematically probing the target's defenses and trying different tactics to see what will work. The hackers are creative, and they pay close attention to results. When one tactic is blocked, they respond immediately with something different.

A recent ATO (Account Takeover) attack against one of our customers is a good example of this. This is a prominent company with a high perceived value for successful ATOs. Thus, the attackers were persistent in their attempts to evade detection and take control of user accounts.

This screen shot shows the first phase of the attack. A single login form received 262k requests over five days. Although the requests themselves were (obviously) mass-generated, it was clear that there was human orchestration going on. Here are some of the tactics that the attackers used.

(continued on next page)

Tactics used during this ATO

- **Moderate rate of requests**: At an average of 50,000 requests per day, the rate was moderate enough to try to stay 'under the radar' and avoid triggering a DDoS incident response, while still allowing the attackers to attempt a worthwhile number of ATOs.
- **Credential cracking**: The incident began as a straightforward ATO attack based on a password dictionary (a list of the most commonly used passwords) to try to crack user credentials and steal accounts.
- **Credential stuffing**: After the attackers realized that cracking would not be successful, they changed to credential stuffing instead (i.e., iterating through a list of full credential sets presumably stolen from other sites. Because many web users still reuse the same credentials across multiple sites, a certain percentage of the login attempts will usually be successful). This type of attack is harder to detect, because each user name is only attempted once, and the passwords are more varied as well.
- **IP address rotation**: Early in the incident, the attackers began using a different IP for every request.
- **ISP rotation**: When their IP rotation failed, the attackers also started using a global pool of ASNs.
- **Further variation**: As the attack proceeded, we saw a lot of diversity in the tactics being used. The attackers tried a variety of user agents, language & locale parameters, and other characteristics, attempting to make their requests appear to be unique and unrelated (to avoid being rate-limited by our security platform).

Aftermath

The tactics used in this incident would have been successful against many—perhaps even most—targets. Robust rate limiting is vital to defeating brute-force assaults, but many web security solutions only offer basic capabilities, such as counting the requests from each IP. Those solutions would have failed to block this attack.

Additionally, we noticed that the attackers had an impressive granularity in their toolset. They were able to fine-tune a wide variety of parameters in the requests being generated, and they were methodical and thoughtful in the tactics that they tried.

The Reblaze platform provides advanced capabilities which can detect and block brute-force attacks according to request content, individual parameters, combinations of parameters, the *number* of combinations of parameters, and more, all with customizable responses. We were able to track and block their efforts.

This incident had multiple phases, as the attackers tried different tactics and our security team deployed immediate countermeasures. Eventually, they gave up.