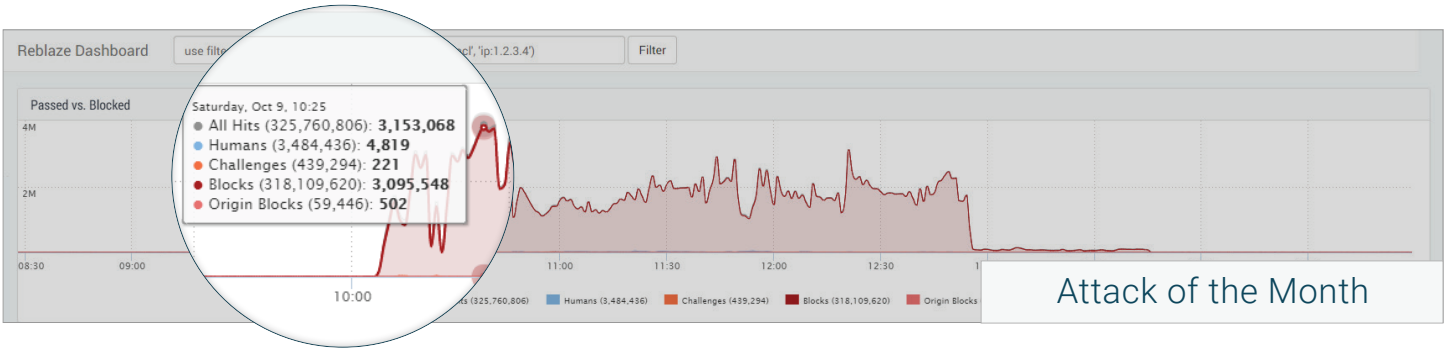


Attack of the Month

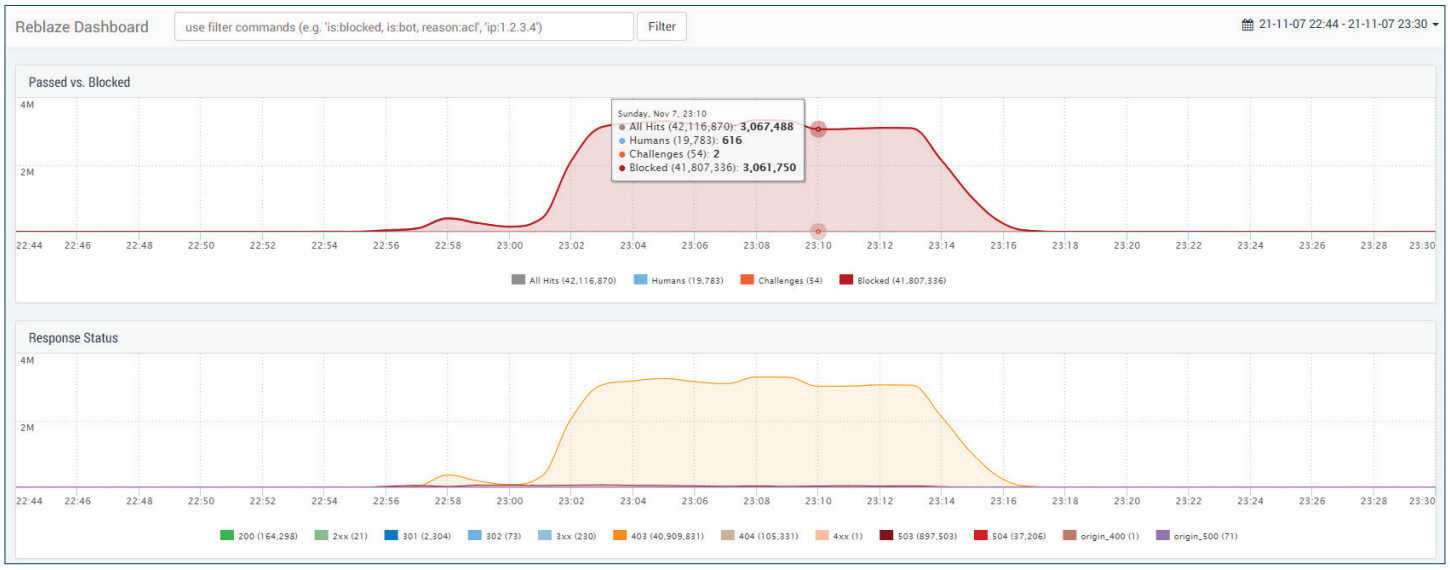
"Whitelist Yourselves for Black Friday"

November 2021: A new form of DDoS extortion

DDoS extortion usually begins with a message from the attacker, threatening an attack unless an immediate payment is made. However, from the attacker's perspective, there are several drawbacks to this.

- The recipient doesn't know if the attacker is serious, or merely sending empty threats with no intention of following through.
- The recipient doesn't know if the attack, if it did occur, would be large enough to overwhelm their defenses.
- Pre-attack messages also include some administrative overhead. The hackers must use some version of CRM; they must keep track of messages sent, responses received, demands that were paid or refused, etc., while organizing and timing everything properly. Sometimes this process breaks down. (We recently saw an incident where the "warning" didn't arrive until after the attack occurred.)

This attack contained a creative way to solve all three of these problems, by building the message into the attack itself.

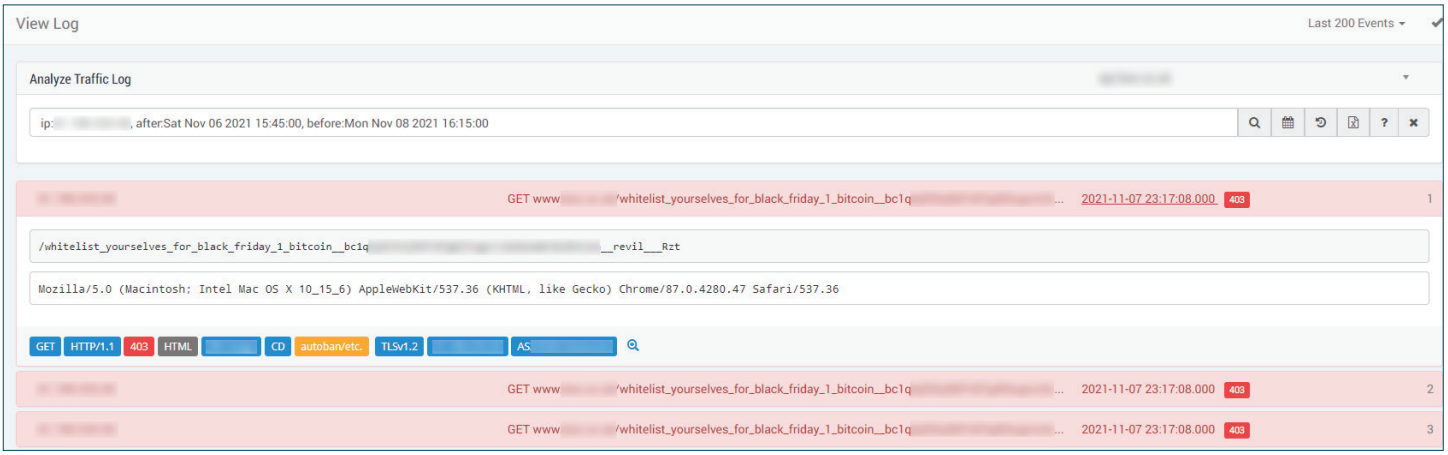


This incident was a respectable size, with a peak slightly above three million requests per minute. Over a twenty minute period, 42 million requests were received.

(continued on next page)

The Reblaze platform provides full traffic transparency, with the ability to drill down into individual requests. Doing so for this attack revealed something interesting.

“Whitelist yourselves for Black Friday”



Private customer info and the attacker’s bitcoin account are redacted

The attacker was sending GET requests to a (non-existent) URL on the target’s site:

<target domain>/whitelist_yourselves_for_black_friday_1_bitcoin_<attacker’s bitcoin address>_revil_Rzt

So, this attack was designed to:

- Knock the target’s site offline for a brief period in order to demonstrate the attacker’s abilities.
- Threaten a much more severe attack (a DDoS during Black Friday, which can be very costly for an online retailer) during the victim’s postmortem analysis.
- And include the extortion demand and payment details in the attack itself. Supposedly, by paying the attackers one bitcoin, the target could “whitelist” their organization, i.e. become exempt from a Black Friday attack.

If the attack had succeeded, this approach would have been a tidy way for the attackers to solve the problems mentioned earlier.

Aftermath

Sending messages to the target as part of the attack itself is one of the more imaginative tactics we’ve seen recently. Unfortunately for the attackers, despite their creative approach, their attack was a failure.

(Reblaze automatically blocked the DDoS traffic before it reached our customer’s servers. In fact, our customer didn’t even realize that the attack had occurred. Our SOC team noticed it in the logs, and mentioned it to them later.)