ERT THREAT ALERT

Tsunami SYN Flood Attack

Overview

Radware's Emergency Response Team (ERT) has detected a brand new technical attack technique that has the potential to challenge a vast majority of current security solutions. Of note, this new type of SYN flood attack:

- Has been witnessed numerous times in the wild and has been successfully stopped leveraging non-traditional protection mechanisms.
- Has been designed to quickly overwhelm BOTH defenses and systems within seconds.
- Differs from classic SYN flood attacks in three fundamental ways: data is contained within each packet; the length of each packet and thus overall attack size; and the network range involved.

To learn more about the exact characteristics of this attack, potentially affected technologies, and initial recommendations for protection please read the following ERT threat alert concerning the 2014 Tsunami SYN Flood Attack.

Classic SYN Flood Attack

The SYN flood is one of the oldest attacks in the textbook yet still a common and dangerous attack even today. The idea behind the attack is that SYN packets – which are easy to generate – consume resources from TCP stacks and stateful devices. Those resources can be consumed quickly and then cause a denial-of-service (DoS). With a SYN flood each packet tries to disguise itself as a legitimate SYN packet and is therefore very small and doesn't contain data.

Today, mature technologies exist to fight SYN floods. These include 'SYN cookies' which won't allow SYN requests to consume resources before the handshake is fully made and the client also sends back the third and last 'ACK' packet. Since SYN flood packets are small they commonly cause a DoS to servers and stateful devices even before they reach a high bandwidth and saturate the internet pipe.

Tsunami SYN Flood Attack

Recently the ERT detected a new type of SYN flood. This exotic attack was seen within a 48-hour period, in two different targets located on other side of the globe. The common characteristic amongst both attacks is that the SYN packets weren't empty. The SYN packets contained data – about 1000 bytes each per packet, and therefore the bandwidth footprint of these attacks was enormous. In both cases an entire network range was hit with the size of the attack reaching 4-5Gbps. Thus, this new type of SYN flood attack was now more likely to saturate the internet pipe of the victim.

As mentioned, common SYN packets don't contain data. Actually the RFC doesn't object to such packets and some applications may even use them but it is very rare. It seems that the intention of the attack here was to find a new method to carry a "tsunami-like", volumetric attack over the TCP protocol. Nowadays we are mostly accustomed to UDP-based volumetric attacks: DNS, NTP and CHARGEN reflected floods are at the top of the list. However, attackers are always looking for new vectors and delivering a tsunami-like attack over TCP can present a new danger. When you have an NTP UDP flood on your site, sometimes it is enough to just block this traffic at the router's ACL level. With a TCP volumetric flood on the web server organizations simply won't close that port.

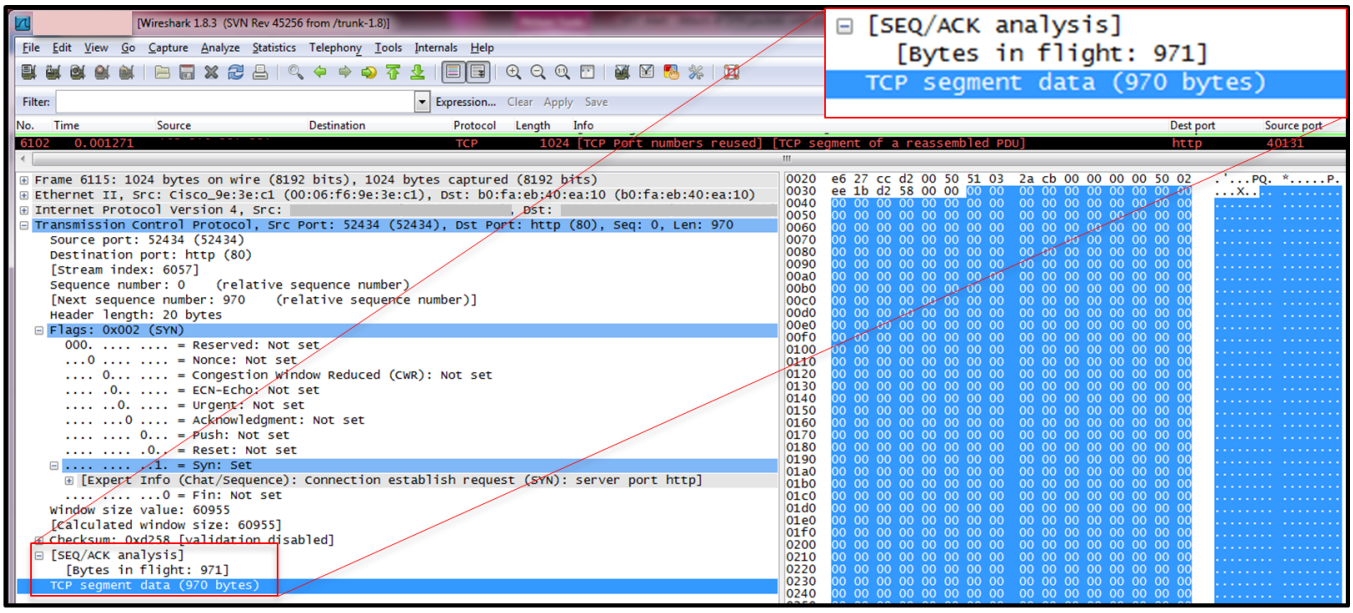

Figure I: The SYN packet contains 970 bytes of data

Unlike classic SYN floods the Tsunami SYN Flood Attack is more likely to impact the internet pipe before it impacts other stateful devices (such as firewalls) and servers. Therefore, to mitigate it you will need to have cloud protection located before the organizational internet pipe.

The ERT further observed that some attacks weren't designated against a specific asset and port but were hitting an entire network range. This additional variant is probably added to make the attack even harder to identify and mitigate.

Industry Recommendation

The ERT recommends that organizations verify that their mitigation solution can block the Tsunami SYN Flood Attack. Since the attack is volumetric the mitigation point must also be in the cloud to prevent internet pipe saturation.

Radware Customer Recommendation

Radware customers using the DefensePro product are protected against the Tsunami SYN Flood Attack. For full protection please make sure the following mechanisms are enabled.

- SYN Protection
- BDOS – SYN Flood Protection

In addition to automatic mitigation technologies, a new signature dedicated to this kind of attack (DOSS-tcp-syn-withpayload) will be published after testing and validation. The signature will provide an additional layer of defense and will accurately detect the attack.

Customers that are using Radware's DefensePipe cloud service are also fully protected against internet pipe saturation. Customers using alternative solutions are encouraged to validate that the alternative solution will be able to mitigate the Tsunami SYN Flood Attack. Customers without cloud protection are encouraged to consider this as an option for protection against this attack vector as well as other volumetric attack vectors that threaten the internet pipe.