Untitled

Dyn Analysis Summary Of Friday October 21 Attack

OCTOBER 26, 2016 **SCOTT HILTON**

Key Findings:

- The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
- Dyn confirms Mirai botnet as primary source of malicious attack traffic.
- Attack generated compounding recursive DNS retry traffic, further exacerbating its impact.
- Dyn is collaborating in an ongoing criminal investigation of the attack and will not speculate regarding the motivation or the identity of the attackers.

Analysis Summary:

The Distributed Denial of Service (DDoS) attack Dyn sustained against our Managed DNS infrastructure this past Friday, October 21 has been the subject of much conversation within the internet community. When the attack first happened our first priority as a company was to mitigate the attacks and limit its impact on our customers. As we have said before, and will continue to say, we thank our customers and the internet infrastructure community for their support during and after these attacks.

During the attack and over the following weekend, Dyn issued a statement and provided extensive comment to the media to keep the public informed. When services were restored to normal, we had the opportunity to conduct additional

analysis of the event. This statement provides a more detailed timeline of the event and a summary of our analysis. That being said, with respect to our customers and the ongoing investigation, Dyn may withhold some information. Additionally, Dyn will not speculate or comment regarding the motivation or the identity of the attackers.

On Friday October 21, 2016 from approximately 11:10 UTC to 13:20 UTC and then again from 15:50 UTC until 17:00 UTC, Dyn came under attack by two large and complex Distributed Denial of Service (DDoS) attacks against our Managed DNS infrastructure. These attacks were successfully mitigated by Dyn's Engineering and Operations teams, but not before significant impact was felt by our customers and their end users.

The first attack began around 11:10 UTC on Friday October 21, 2016. We began to see elevated bandwidth against our Managed DNS platform in the Asia Pacific, South America, Eastern Europe, and US-West regions that presented in a way typically associated with a DDoS attack. As we initiated our incident response protocols, the attack vector abruptly changed, honing in on our points of presence in the US-East region with high-volume floods of TCP and UDP packets, both with destination port 53 from a large number of source IP addresses. The abrupt ramp-up time and multi-vectored nature of the attack, led to our Engineering and Network Operations teams deploying additional mitigation tactics on top of our automated response techniques. These techniques included traffic-shaping incoming traffic, rebalancing of that traffic by manipulation of anycast policies, application of internal filtering and deployment of scrubbing services. Mitigation efforts were fully deployed by 13:20 UTC; the attack subsided shortly after.

At roughly 15:50 UTC a second attack began against our Managed DNS platform. This attack was more globally diverse, but employed the same protocols as the first attack. Building upon the defenses deployed during the earlier attack and extending them globally, we were able to substantially recover from the second attack by 17:00 UTC. There was residual impact from additional sources that lasted until approximately 20:30 UTC.

A number of probing smaller TCP attacks occurred over the next several hours and days; however, our mitigation efforts were able to prevent any further customer impact.

During a DDoS which uses the DNS protocol it can be difficult to distinguish legitimate traffic from attack traffic. For example, the impact of the attack generated a storm of legitimate retry activity as recursive servers attempted to refresh their caches, creating 10-20X normal traffic volume across a large number of IP addresses. When DNS traffic congestion occurs, legitimate retries can further contribute to traffic volume. We saw both attack and legitimate traffic coming from millions of IPs across all geographies. It appears the malicious attacks were sourced from at least one botnet, with the retry storm providing a false indicator of a significantly larger set of endpoints than we now know it to be. We are still working on analyzing the data but the estimate at the time of this report is up to 100,000 malicious endpoints. We are able to confirm that a significant volume of attack traffic originated from Mirai-based botnets.

Early observations of the TCP attack volume from a few of our datacenters indicate packet flow bursts 40 to 50 times higher than normal. This magnitude does not take into account a significant portion of traffic that never reached Dyn due to our own mitigation efforts as well as the mitigation of upstream providers. There have been some reports of a magnitude in the 1.2 Tbps range; at this time we are unable to verify that claim.

Dyn will continue to conduct analysis, given the complexity and severity of this attack. We very quickly put protective measures in place during the attack, and we are extending and scaling those measures aggressively. Additionally, Dyn has been active in discussions with internet infrastructure providers to share learnings and mitigation methods. We've also been the beneficiary of analysis by the internet infrastructure and monitoring community, and sincerely appreciate the support.

This attack has opened up an important conversation about internet security and volatility. Not only has it highlighted vulnerabilities in the security of "Internet of Things" (IOT) devices that need to be addressed, but it has also sparked further dialogue in the internet infrastructure community about the future of the internet. As we have in the past, we look forward to contributing to that dialogue.

On behalf of Dyn, I'd like to again reiterate our appreciation for the outpouring of support and offers of assistance from our customers, partners and internet infrastructure stakeholders.