Michael Guidry
January 17, 2017
Unified Defense Technologies, Inc.
mike@unifieddefense.net

Poison Windows — DNS amplifications and their unforeseen side effects

This is the second of a series of papers that I'm releasing which will explain how security mitigations become new attack vectors. I hope that some people will have some fun with this release without causing too much damage as a byproduct. I believe it has many uses in anyones hacking campaigns.

Domain Name System (DNS) is the literally life blood of the world. You will not perform any type of transaction on earth in 2017 without relying on it. Mobiles, endpoint devices, and all computers worldwide perform hundreds of queries daily. Several years ago people had recognized that the nature of DNS allowed for several attacks. DNS poisoning, and amplification are the two most important attacks. The most recent public poison attack worked a hundred percent of the time. It was a logic issue with one hostname being able to report an IP for another hostname. Amplification is the more recent issue that pretty much everyone has to watch out for. Modifications to the code base had taken place to ensure the attacks wouldn't come from machines using DNS software. ISPs even scan their customer base to ensure patch usage.

DNS Distributed Denial of Service (DDoS) mitigation itself creates a major attack vector. DNS is considered fragile. It is an extremely old protocol, and nobody has found a good way to upgrade it. It is right alongside Border Gateway Protocol (BGP) in the way that it should be revamped while globalization increases, and the internet becomes even more important in everyones lives. It would be smart if the United Nations comes together to work out a plan to allow replacing with more secure, and robust software. I won't hold my breathe.

Administrators around the world have been applying patches in a pretty slow form since a lot of these machines are servers, or embedded devices. DNS amplification works by sending requests for zone files with large amounts of information to a name server while faking the IP address of a target. Zone files are a single file that contains all hostnames for a domain. It causes that server to respond with that packet to a target sometimes amplifying the initial packet several times over. Its quite a nice attack in reality. DNS had some revamping to add a limitation. Rate limiters were put into place to allow blocking computers which requested too many times. We are all saved. Or not…

DNS poisoning is a technique used to modify the IP addresses of another server's host names on a target computer. It essentially lets you change the phone number of the destination you wish to manipulate. DNS uses a protocol which doesn't require more than one packet before performing the action your requesting. The Hypertext Transfer Protocol (HTTP) is different because the computer communicating over it has to receive packets before the web server performs the actions. This is a quick example of the difference between the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP). DNS is a stateless UDP protocol which is faster since it doesn't wait for several communications, however it is a bit less secure if not developed properly.

DNS queries have identification numbers which allows the requester to verify that the server is responding to the correct packet. Its purposes are for separation, security, and possibly logging. Security is the way it is used while being exploited by this attack. It means that the client is choosing a number for the identification that shouldn't be possible to guess before it receives its response. It works great, and every few years a cryptographer finds a nifty way of manipulating it. I won't comment on analysis required for prediction. It is a different side of the attack vector. It will vary from operating system as well.

Large numbers of DNS servers worldwide now perform verification to ensure they do not take part in these amplification attacks. Unknowingly, they have become some of the most vulnerable nodes within the entire internet infrastructure. Any company using these mitigation techniques have become vulnerable to these attacks. Targets may begin receiving poisoned responses from their networks due to the amplification protection.

DNS poisoning is a manipulation of the protocol to modify another DNS hostname's IP addresses. The query identification number must be predicted, and sent back faking a query from the server to a target. It will allow you to do things like replace Google with your own IP address on a target. You pick a target, and the hostname you wish to poison. You use some tactic to have that target request from the hostname's server for its IP address for that entry. One way would be to locate the DNS server that the target uses, and then manually request queries on it. You could even fake the requests from the target directly except certain situations where the router would block you. If you are able to respond fast enough with the particular identifier then you have committed a successful poisoning attack. Its only useful if your able to accurately guess the query identification number within a really small time frame such as milliseconds to seconds.

The issue is determining the query identification number within the small amount of time it takes for that DNS server to find the hostname in its own records, or requesting it from another host. It suddenly becomes a pretty difficult task. This is where this attack vector really matters. Wouldn't it be nice to have ten seconds? That could be 20-30 times the original small amount of time you had to respond. The odds can start to help in your favor. Imagine if you just continued to fake those queries causing the amplification protection to activate mechanisms to ignore your target completely? You suddenly have increased that time to infinite.

Lets say you do not wish to perform all of this analysis, prediction, etc. You have a second more subtle option. If you wanted to attack a company, or target then you can begin to have them blocked from various hostnames. You could use things such as anti virus companies, Microsoft, Apple, or even Google. If their anti virus stops updating then you could theoretically continue the attack infinitely. It depends on the software although this attack may block that company from submitting your hacking tools to companies for analysis. It would give you time to remove the evidence from their systems if you could accurately block all of the important hostnames that are used within the security industry.

Fixing this new 'poison window' attack is impossible without redesigning DNS DDoS mitigations. It would require CPU intensive tasks for further verification. Its possible that its infeasible to fix both issues. Blocking spoofed packets on routers is the way to go. I highly doubt a large portion of the internet would ever apply these tactics. It might even disrupt some protocols, or services.