ERT Threat Alert
Masked Amplified DDoS
May 17, 2018

Background

Security researchers have observed[i] a new evasion technique - source port obfuscation - used for conducting denial-of-service attacks. It delivers amplified payloads through nonstandard ports. This evasion technique was used in two attacks in April when perpetrators masked the source port of the amplified denial-of-service attack. The first was an SSDP Amplification attack where the SSDP payload was delivered from an unexpected source port. Typically, SSDP Amplification attacks originate from port UDP/1900, but in this case, a small portion of the payload came from other source ports. In the next masked amplification, the attackers used the NTP protocol. NTP amplified payloads originate from port UDP/123, but once again, the team observed payloads coming from nonstandard ports.

Attack Methods

Attackers are exploring the use of Universal Plug and Play (UPnP) to mask their amplification attacks so they can deliver amplified payloads via nonstandard ports. UPnP is a protocol used to simplify the discovery of other devices on a local network. For example, if a user plugs a device such as a printer into the network, the devices will automatically configure itself, acquire an IP address and announce its presence to the network so that the appropriate connection can be made. The UPnP-IGD protocol – which is based on SOAP/HTTP - is being used to add port mapping to a UPnP enabled router. Unfortunately, very few routers verify the authentication or the forwarding process. This allows attackers to use the router to redirect incoming internet IP addresses to other IP addresses. The attackers are able to mask the incoming amplified packets and defeat traditional mitigation solutions who rely on legacy detection methods.

According to the researchers, the attacker must first search the internet for vulnerable routers that expose the rootDexc.xml file that holds the port mapping configurations of the device. Using automated techniques, the attacker can quickly scan for vulnerable devices and use an HTTP request to access this file. Once the device has been accessed, the attacker adds a port-forwarding rule with `AddPortMapping`. UPnP-IGD uses a SOAP request (i.e. HTTP Post) to the device with a SOAP envelope containing the AddPortMapping setting. By default, most routers listen and process UPnP HTTP requests from the WAN interface without authentication. Hence, the modified device is now ready to mask amplified attacks by changing the source port of the amplified attack traffic as it relays through the device.

Amplification Methods

NTP: Attacker sends spoofed NTP packets containing monlist request code to a list of vulnerable NTP servers. Monlist is a command requesting a list of the last 600 hosts who connected to the addressed NTP server. Consequently, the NTP server sends a large amplified reply to the spoofed IP address (the victim), thus flooding their network.

DNS: A DNS amplification attack is when the attacks sends a “ANY” DNS name lookup request to a list of open DNS servers with the source IP address spoofed to be the victim’s IP address. The DNS server responds by sending all known information about the DNS zone to the victim’s IP address, resulting in an amplified attack.

SSDP: When an attacker sends spoofed packets containing the victim’s IP address to a list of active UPnP devices. The spoofed packet with an `ssdp:rootdevice` or `ssd:all` sent to each UPnP device on the list replies back with an amplified answer to the victim’s machine that contains all the services on the device.

Memcache – A Memcache amplification attack is a UDP volumetric denial-of-service attack whereby the attacker performs two malicious tasks similar to that of a DNS attack. First, the attacker builds an amplification list of vulnerable Memcache servers with UDP port 11211 exposed. In the second step, the attacker will send a spoofed GET request to the vulnerable Memcache servers on the amplification list. As a result, the Memcache servers will reply to the GET request and forwards an amplified response to the spoofed IP address.

Targets

UPnP enabled devices with rootDesc.xml exposed are being targeted to launch masked amplified denial-of-service attacks.

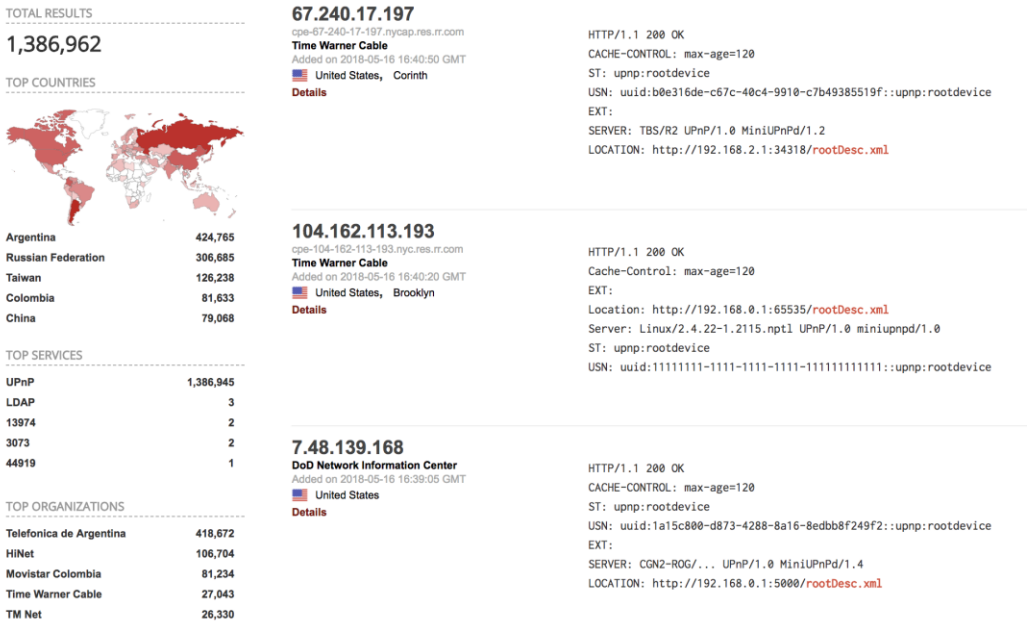

Figure 1: Shodan results for “rootDesc.xml”

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Protecting Against Source Port Obfuscation

System administrators are advised to disable UPnP-IGD automatic port forwarding in the router to prevent the abuse of vulnerable devices. Vendors who produce devices with UPnP/PNP must block unauthorized access by default.

Radware Customers

Source port identifications is only one of the many parameters Radware’s Network Behavioral Analysis detects and creates a signature to block attacks in real time before it affects the network.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you’re under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button.”

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] https://www.imperva.com/blog/2018/05/new-ddos-attack-method-demands-a-fresh-approach-to-amplification-assault-mitigation/