Problem/Issue Identification and Description

**Submittal Date** (02/07/2022): **PIM # 142**

**Company(s) Submitting Issue**: 10x People / Inteliquent

**Contact Name(s)**: Lisa Marie Maxson and Cheryl Fullerton

**Contact Number(s)**: +1 (303) 522-7171 /

**Email Address:**  lisamarie@10xpeople.com, Cheryl.Fullerton@Inteliquent.com

**(NOTE: Submitting Company(s) is to complete this section of the form along with Sections 1, 2 and 3.)**

1. **Problem/Issue Statement:** (Brief statement outlining the problem/issue.)

VoIP service providers are susceptible to IP network attacks, as evident by recent DDoS attacks (see definition in section F below), both domestically and abroad in the last several months. In order to restore service to end-customers, porting was required to move customers to unimpacted networks, to resolve these customer outages. The current NPAC transaction rates defined in the FRS specification are insufficient to support the porting volumes required. There were no provisions for exceeding the documented transaction rates.

1. **Problem/Issue Description:** (Provide detailed description of problem/issue.)

A. Examples & Impacts of Problem/Issue:

When large VoIP carriers are under DDoS attacks, network traffic must be rerouted for calls to complete. Rerouting (via porting) the traffic to another unimpacted service provider’s network as quickly as possible is required to enable call completion, for both inbound and outbound calling. Porting allows for network routing to change, by giving a different LRN for call routing.

In one attack, due to a large number of impacted customers, including hospitals and other essential services, porting had to be completed quickly and in large volumes. Unfortunately, while other carriers were willing to assist in porting customers, the required transaction rates exceeded NPAC transaction rates defined in the FRS specification. Customers unable to port were left without or with limited service from the network service provider under attack despite best efforts by both the impacted service provider and other industry service providers.

Additionally, there can be impacts to service providers not directly involved in the ports related to this situation. These include but are not limited to fines for not meeting QoS requirements by PUCs (e.g. AL, FL and others) and direct and indirect costs related to increased rate of porting volume.

B. Frequency of Occurrence:

DDoS attacks against four VoIP providers are publicly known to have occurred in the fourth quarter of 2021. Malicious actors are continuing to work to attack networks across the globe. Government agencies such as the FBI, CIA, and NSA are working to prevent attacks; however, there is no silver bullet to prevent future attacks. While the frequency of future attacks is unclear, we must be prepared to react and to prevent customer and essential services outages.

(*Source: Nexus Guard*) The COVID-19 pandemic brought a massive increase in cybercrime. The beginning of 2020 recorded a 2.5 times increase to Q1 of the previous year, and an almost 4.5 times increase compared to Q4 2019.

(*Source: Dark Reading*) Researchers recorded approximately 2.9M DDoS attacks in the first quarter of 2021, marking a 31% increase from the same period in 2020. This will likely result in exceeding the 10M attack threshold recorded in 2020.

1. NPAC Regions Impacted:

 Mid Atlantic \_\_\_ Midwest\_\_\_ Northeast\_\_\_ Southeast\_\_\_ Southwest\_\_\_ Western\_\_\_

 West Coast\_\_\_ ALL X

D. Rationale why existing process is deficient:

Currently, service providers are limited to the transaction rates specified in the FRS to prevent the overwhelming of the ecosystem, specifically the LSMS systems that update the network elements for call routing.

Additionally, there is not a documented industry process for urgent/emergency situations that warrant higher porting volumes with the NPAC or the ecosystem as a whole.

Carriers affected by any attack will be the first to know, and empowering them to work with other Carriers, with a level of urgency that all Carriers understand, will allow restoration of service to customers in the most timely fashion. Emergency situations should allow Carriers to utilize the most efficient process, regardless of whether this is occurring during or after regular business hours.

1. Identify action taken in other committees/forums:

The NANC NAOWG has requested that the NPIF discuss this PIM and provide feedback.

F. Any other descriptive items:

A Distributed Denial of Service (DDoS) attack is a subclass of a Denial of Service (DoS) attack. A DDoS attack involves multiple connected online devices, collectively known as a botnet, that overwhelm a target network with fake traffic. Cybercriminals flood the network with so much malicious traffic that it cannot operate or communicate in a normal fashion. This causes the site’s normal legitimate packets to come to a halt.

In the case of a VoIP network DDoS attack, the influx of fake traffic prevents calls from being routed and completed. Connections that might be established can be dropped or experience severely reduced voice quality.

1. **Suggested Resolution:**

Raise existing throughput requirements to allow for increased porting volumes.

Consider exceptions to transaction volume limitations in these situations to allow higher porting volumes.

Put M&P in place for the NPAC and the industry for when these situations arise.

1. **Final Resolution:**

This PIM resulted in the creation of a Best Practice (#78 – Service Outage Prevention and Mitigation).

**NPIF (only)**

PIM #: 142 Final Resolution Date: 11/08/2022

Related Documents: BP 078

Issue Resolution Referred to: ATIS NGIIF, NRSC

Why Issue Referred: While issue was being worked by SOS (Service Outage Support) sub-team of NPIF, it was decided to work with other industry fora where DDoS issues may have been discussed and alternate solutions developed.