Research Note

June 2024

Cat and Mouse with DDoS

DDoS market environment and remediation, seen through the data and eyes of Nokia Deepfield

Author: Grant Lenahan - Principal Analyst

www.appledoreresearch.com

Appledore
RESEARCH

Published by Appledore Research LLC • 44 Summer Street Dover, NH. 03820

Tel: +1 603 969 2125 • Email: info@appledorerg.com• www.appledoreresearch.com

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Appledore Research LLC independently of any client-specific work within Appledore Research LLC. The opinions expressed are those of the stated authors only.

Appledore Research LLC recognizes that many terms appearing in this report are proprietary; all such trademarks are acknowledged, and every effort has been made to indicate them by the normal USA publishing standards. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Appledore Research LLC maintains that all reasonable care and skill have been used in the compilation of this publication. However, Appledore Research LLC shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising because of the use of this publication by the customer, his servants, agents or any third party.

Publish date 28 June 2024

Cover image: Bing image creator/Robert Curran

Executive Summary

Distributed Denial of Service attacks (DDoS) have been a tremendously lucrative activity for bad actors. Being lucrative also takes many forms—from state sponsored disruptions of political or economic apparatus, to the far more common but mundane ability to ransom for profit. Regardless, it has become a major segment unto itself, with the ability to create havoc and significant cost not only for the attack victim (typically an enterprise or government agency) but also for the serving network.

This research note combines a look at two developments; the technological evolution of DDoS, and the corresponding and resulting evolution of the Nokia Deepfield Defender DDoS security solution, rooted in their Deepfield network analytics solution, and the Nokia FPx series of fully programmable router chips.

Appledore greatly appreciates the periodic and data-rich updates that the Deepfield team provides to us (and which forms part of the basis of this note) and to many in the industry. More information may be found here (2023 data, 2024 to be published next quarter).

We will cover the cat-and-mouse game that is going on, as DDoS becomes increasingly sophisticated and exploits unexpected resources on the web to tilt attack economics in bad actors' favor. We will also discuss the counter measures this makes necessary. We will continue with the look at how Nokia Deepfield is positioning their recently expanded countermeasures. Finally, we will conclude with implications for what all this means for network operator buyers.

Spoiler alert: sometimes terrible developments contain a business opportunity. Appledore believes this is one of those times, in which CSPs should position themselves with technology capable of delivering a superior defense, and doing so at a cost that allows for it to be turned into a profitable network-based service.

DDoS In Brief (History, Primer on remediation, …)

DDoS attacks are launched using various methods that overwhelm a target's serving network and computer infrastructure rendering it unreachable and/ or inoperable. The earliest attacks were brute force queries. The bad news is that they were unexpected and therefore worked. The good news was multi-faceted:

- They could be fingerprinted and therefore identified
- They demanded that the attacker spend money on sufficient capacity to overwhelm – meaning the attack as costly and the playing field somewhat fair
- They mostly came from predictable places, outside "respectable" networks

Because they came from outside the target's network, this also meant that attacks came from beyond the network's edge, and therefore the best place to stop an attack, before it could overwhelm either the target or parts of a serving network, was at the network ingress point: squelch it before it could do much harm. We will expand on these shortly.

The first solutions used an approach that will be familiar to anyone who has loaded anti-malware software onto a device: create dedicated software that identifies and cleanses traffic, and load a constantly updated list of fingerprints that identify the characteristics of that DDoS/attack data so that it may be segregated and “cleansed”. You can’t block what you cannot identify.

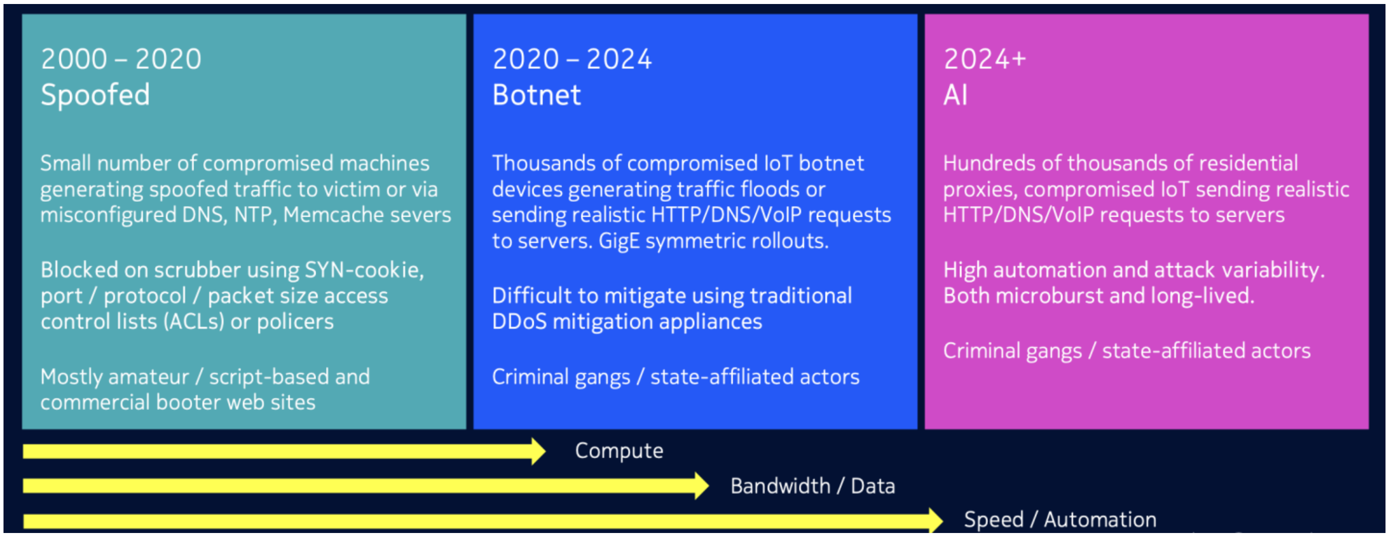
Often these dedicated “cleansing” appliances were racks of equipment in convenient but centralized (therefore remote) locations. All data that contained fingerprinted traffic was routed there so that the bad traffic could be terminated, and the good traffic forwarded to its intended recipient. This allowed for improved utilization of expensive cleansing equipment, but resulted in high backhaul costs, generally slow identification of new threats (or morphing ones, but few did in the early days), and also created significant delays for actual traffic that was backhauled, cleansed and re-forwarded. But that was the norm.

DDoS Market Evolution – The Cat Continues to Innovate

And here is where the cat-and-mouse game begins. The **bad actors, as is typical, have not been stagnant**. Not content to be terminated, DDoS has constantly evolved to evade detection and overwhelm remediation.

Nokia’s Deepfield team (like other DDoS solution specialists) has been following the shift in DDoS sources and methods carefully, and sharing the update with analysts, customers and CSP leaders periodically. While emphasis shifts somewhat depending on who’s analysis one uses, **we will anchor our analysis on Nokia’s recent data**, since it is the most comprehensive and newest we have seen.

Figure 1: Simplified DDoS evolution timeline, courtesy Nokia



2000 – 2020
Spoofed

Small number of compromised machines generating spoofed traffic to victim or via misconfigured DNS, NTP, Memcache severs

Blocked on scrubber using SYN-cookie, port / protocol / packet size access control lists (ACLs) or policers

Mostly amateur / script-based and commercial booter web sites

2020 – 2024
Botnet

Thousands of compromised IoT botnet devices generating traffic floods or sending realistic HTTP/DNS/VoIP requests to servers. GigE symmetric rollouts.

Difficult to mitigate using traditional DDoS mitigation appliances

Criminal gangs / state-affiliated actors

2024+
AI

Hundreds of thousands of residential proxies, compromised IoT sending realistic HTTP/DNS/VoIP requests to servers

High automation and attack variability. Both microburst and long-lived.

Criminal gangs / state-affiliated actors

Compute

Bandwidth / Data

Speed / Automation

From its single source, typically offshore roots, the first **major shift in DDoS launch characteristics** began ~ 4+ years ago, with the shift from self-contained attack servers / clusters to methods that took control of armies of Internet “Things”. This shift was foundational:

- It allowed attackers to cloak themselves behind otherwise innocuous looking sources via hijacking and spoofing.
- It allowed an increase in volume, and a many-orders-of-magnitude increase in source addresses
- Since most of those “things” are located within the target’s region, suddenly attacks came from within the targets serving network and from quote friendly networks.
- By implication, the threats were not always beyond the target’s networks edge—and therefore some remediation must take place within the network
- Hijacking IoTs shifted the economics in bad actors’ favor, by allowing them to utilize (free) attack resources and network connectivity they do not pay for.

The **implications** are also several; remediation capacity must increase; remediation capacity must be more distributed; cost of remediation increases; no longer can a small number of IP or other identities be used to identify DDoS traffic.

A second shift is underway now, driven by two technological innovations: the **application of AI** to make attack vectors adaptive to counter measures, And the addition of powerful residential proxies to the existing IoT army, providing much greater compute capacity to perform complex activities that simulate legitimate traffic.

There are **clear implications** for targets and their networks. First, it is no longer always possible to identify good versus bad traffic with header inspection and simpler fingerprinting; **DPI** is required for identification in more traditional CPU logic is necessary for remediation. At the same time, the AI “innovation” allows attacks to be adaptive to countermeasures; constantly morphing as necessary. The implication is that identification **characteristics can no longer be pre identified**. With the strong capabilities of these proxies, combined with AI's ability to constantly evolve and evade countermeasures, the **countermeasures must be equally adaptive**. All of this of course leads to cost and complexity—and therefore demands a sophisticated and highly efficient solution.

Understanding Deepfield’s approach and how it differs from traditional methods

Above we provided a very brief history lesson in DDoS and remediation techniques followed by a summary of how DDoS is evolving. Both of these are necessary as we think about how solutions must evolve and as always how telcos and enterprises need to think differently about the problem.

We find it easiest to think about Nokia's defender solution as having two major components, each of which begins with a slightly unique perspective on technology and how to solve the DDoS problem.

The first component is the Deepfield analytics platform itself. A simple summary is that Deepfield began with the belief that a) data sources could come directly from modern network functions—mostly routers; b) Network traffic could be characterized and fingerprinted through ongoing “crawling” by intelligent agents; and c) this database of traffic sources could be used for myriad applications with the actions carried out not by Deepfield itself but by increasingly intelligent routers in the network. Examples are traffic management and security, but **Deepfield's focus** has increasingly been on **security** in general and DDoS in particular. These constantly updated databases of traffic types, sources, etcetera are the Deepfield "genomes" -- In the security version is the **Secure Genome**. To the best of our knowledge no competitor has such a genome.

The second component—which is crucial to thinking about the operational perspective from Nokia and Deepfield, **is Nokia's proprietary routing silicon family—the FP series of routing chips**. The Nokia FP chips' claim to fame is that they can operate without performance impact even if they are inspecting and conditionally routing/terminating (including DDoS cleansing) 100% of incoming traffic. There is a caveat however: such routing chips do not perform true DPI but inspect headers and packet characteristics -- things that routers do.

There are **operational and cost implications** to the combination of 1) Deepfield as investigation and intelligence and 2) routers as what are effectively policy enforcement points under the control of Deepfield intelligence. First, it means that DDoS traffic may be identified, intercepted, and terminated as close to the source as an FP-equipped[1] router exists. By cleansing inline (on routers), backhaul is eliminated. By eliminating backhaul, latency, delay, and out-of-order packet arrival are eliminated. Nokia also claims that the cost (per unit of volume and throughput) is lower on these highly optimized routers. The claim makes technical sense, since highly specialized chips are typically much more efficient compared to general purpose. Witness GPUs, Neural processors, and 5G layer-1 acceleration chips.

The **downside** of remediation being performed on a routing chip, is that – it's a routing chip and not a CPU or GPU. This has always been a design and optimization tradeoff of the Nokia Defender solution, which has always had minimal application layer remediation capabilities, but provided volumetric leadership and cost leadership (which is particularly important when offering a managed service – more on that later). Presumably this has been an overall advantageous trade off—however the rise of proxy-based attacks complicates this calculus.

It's also worth noting that some CSPs have been hesitant to move off of the use of dedicated scrubbing centers, and have security teams that prefer to manage standalone appliances rather than commingle their work with network routing organizations. Nokia recognized this and introduced an FP5-based DDoS appliance in 2023. We covered that in this report which is worth reading for further background and information on DDoS and DDoS solutions. Yet, preferences aside, there are real advantages to edge-based DDoS mitigation and conditional routing.

[1] Without getting into details Deepfield can also program other brands of routers using industry standard protocols—however as the number and complexity of these rules increases all other routers begin to either drop traffic or operate at a slower rate both of which interfere with capacity planning and impact cost. Further discussion is beyond the scope of this already deep research note.

What's New in Nokia and Deepfield Defender?

Nokia and the Deepfield Defender family have introduced three capabilities to combat the new, proxy-supported, AI supported wave of DDoS. In a nutshell, they announced:

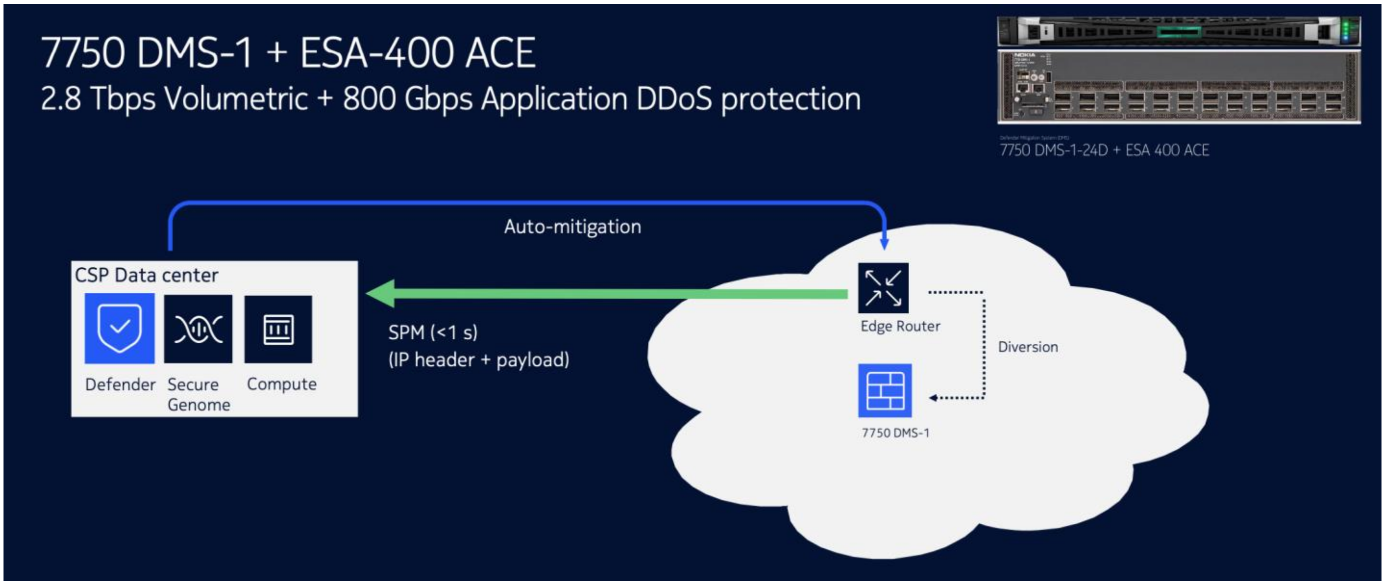
- Within Deepfield, good guys (CSPs) now have their own AI/ML to continuously monitor attacks, detect evasion, and re-tune the remediation.
- Introduction of a new component for the appliance (scrubbing/datacenter-based components) based on GPUs and optimized for interactive application-level countermeasures. This augments the FP5 based 7750 DMS which retains volumetric (router based) performance and cost advantages where it is sufficient
- 3X faster detection and mitigation initiation

The net of this is a claimed 10X scale and speed advantage compared to "as deployed" (legacy) solution – which is no doubt comparing to a moving target, but likely the present day reality in many networks.

The new remediation component is "ACE," which stands for Advanced Countermeasures Engine, a new module that augments the FP5-based DMS volumetric appliance. **This new module provides GPU-based DPI and application-level (interactive) remediation**. Ideally these augment the first line of defense which is in-line, on FP5-based (or third party) routers, as close to the source as possible. At the edge, some traffic is terminated. Other traffic is diverted to the cluster(s) of 7750 DMS with ACE.

The diagram below, from Nokia, illustrates both front line (edge or near edge) actions and secondary actions in a data center using DMS and ACE resources for interactive, application-level attacks.

Figure 2: Nokia 7750 DMS-1 & ACE combine to deliver a 7-layer remediation solution



7750 DMS-1 + ESA-400 ACE

2.8 Tbps Volumetric + 800 Gbps Application DDoS protection

Courtesy: Nokia

Appledore's Analysis

Three issues are raised by the data that underlies this research note:

1. The **constantly rising sophistication** and stakes posed by ever-more-sophisticated DDoS attacks, which can not only impact target enterprises, but also cripple or at minimum disrupt CSP network traffic and operations
2. The relative capabilities and **cost/performance position** provided by **Nokia's family of DDoS** detection and remediation solutions (Deepfield Defender, FP5-based routers, 7750 DMS with ACE).
3. The large **market need for DDoS protection as a service**, and the consequent opportunity for CSPs – which in turn is dependent on the evolving economics of solutions

Appledore has covered the rapidly rising sophistication, and the consequent costs to enterprises and society, of security vulnerabilities. We have underscored the fact that the digitization of the world makes us all more vulnerable and makes the costs higher and therefore the stakes higher. And we have quantified the opportunity for CSPs to remediate "aaS." We refer interested readers to major reports and market forecasts that we produced on network based security here (forecast) and here (market outlook).

In brief, those reports show that the **incremental revenue opportunity for CSP's to provide security as a service is huge**. Moreover, the scarcity of expertise makes it not only a business opportunity but a practical necessity. Industry organizations are recognizing this, with **the MEF** even defining an integrated bandwidth and security bundle as a "secure service."

What is needed however, is a highly efficient remediation infrastructure that can perform at a cost structure below that of the market price for such protection. Thus, our interest in new vendor solutions. Over the last two to three years, we have had too many discussions for our comfort, that had elements of "we would if the economics were better" or "we'd like to jump to more efficient technology, but it doesn't fit our operational model." Both translate to "we have a cost problem and are giving up significant revenue as a consequence."

The rising sophistication of DDoS attacks is a two-edged sword, if you are a service provider. Fundamentally, of course, it is bad -- it is a vampire squid sucking money out of the legitimate economy. Regardless, bad things exist, and **the other edge of that sword is the business opportunity**.

We believe it is imperative that CSPs think not incrementally, but in absolute terms, about what the best technology is to fight DDoS effectively and cost efficiently. They must that this stance because doing so can provide a viable profit opportunity, while doing good. Figuring out "cost efficiently" is, of course, complicated, since one of the key messages of this document is that DDoS is constantly changing and therefore today's solution may not be ideal for tomorrow's world. **We do believe that one size fits none however**, and therefore believe that Nokia's approach, which in effect uses three different methods to remediate based on which one is most efficient for that subset of attack data, is likely a very good approach and one that can be scaled independently as one component of attack data grows relative to others. The three methods we refer to are 1) edge handling on routers, 2) data center handling on router-based appliances, and 3) data center handling using on GPU-based appliances. All under the control of Deepfield analytics and AI.

Turning our attention to the evidence from the market, Deepfield, while remaining a multi-app platform, is doubling down on security. They claim to have more than 80 customers overall, and have added 13 in the last 12 months – all indicating market acceptance. The rationale given by Nokia matches what has been discussed in this document—CSPS are buying faster detection, more accurate detection, and a better cost / performance ratio. They also emphasized that on their existing router-based solutions and router-based appliances, the fine grain handling capabilities provided by FP series chips provides a significant traffic and cost efficiency by minimizing what must be that called to DPI. Appledore underscores that this cost performance ratio implies viable new businesses, and in fact Deepfield validates this with the evidence that some “previously marginal use cases” became economically viable, citing neutral hosts.

In summary, security in general and DDoS in particular are big problems, and getting bigger. Moreover, it is constantly changing. CSPS need to think not only about how they can be as efficient as possible but how they can have a platform that can adapt and react to new innovations as efficiently as possible. We also recommend that CSPs consider how to make this not merely a cost but also a new source of revenues while doing a service to their customers and to society.

Insight and analysis for telecom transformation.

@AppledoreVision

Appledore Research

www.appledoreresearch.com

info@appledorerg.com

+1 603 969 2125

44 Summer Street Dover, NH. 03820, USA