MICRON21 DEPENDS ON NSFOCUS FOR PROTECTION AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACKS

"The NSFOCUS solution has performed flawlessly."

– James Braunegg, Managing Director, Micron21

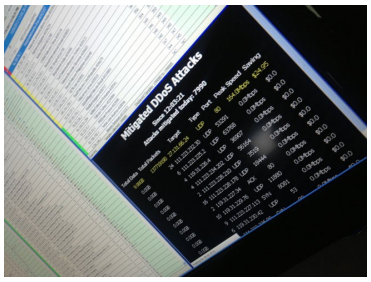
Company Profile

Micron21, a Data center provider based in Melbourne Australia, owns and operates the largest peered network in Australia. Their network consists of six data center locations throughout the world connected to more than 1,500 global networks. This broad reach is the perfect complement to their high performance and low latency infrastructure, designed to scale on demand for their hosting and connectivity services customers. Micron21 offers a fully redundant network that is managed and monitored by their Network Operations Center 24/7 365 days a year, within the only tier certified Data center in Australia.

The Challenge

As Micron21 was building out the network, their hosting customers frequently experienced small DDoS attacks that took them offline. While the Micron21 network was still operational, the end customers experienced service disruption and turned to Micron21 for help. "We started to look at how to stop the attack traffic" said James Braunegg, Managing Director of Micron21, "because these attacks were negatively impacting our customers and our business".

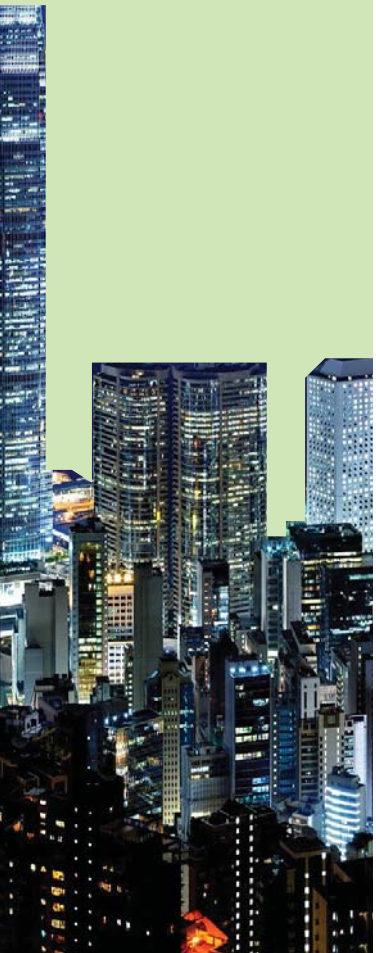
The team at Micron21 initially attempted to filter the malicious traffic using their existing routers but found that the routers quickly failed under the processing load, leading to larger, more significant network-wide outages. The team next turned to firewalls to block the attacks, but these quickly reached capacity and failed due to the number of sessions that needed to be tracked in order to mitigate the DDoS attacks. Micron21 then purchased and installed higher -capacity routers but found that the only way to keep them online was to "null route" or drop all traffic destined to customers that were under attack. This was clearly not a viable solution and the team realized they needed to deploy specialized security that would accurately identify and drop only malicious traffic. Legitimate traffic would continue to be forwarded with no degradation to the end-user experience.



-24/7/365 network monitoring

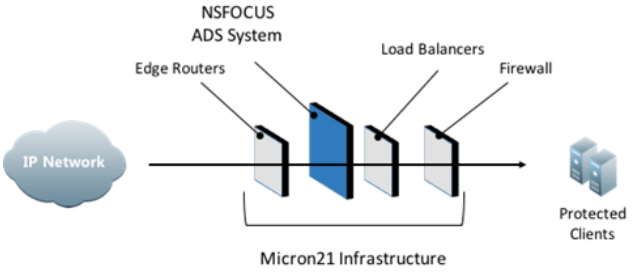
The Solution

h n n t n nt h ne h n n t hn h l
h n u t n t hn e nl ent h u n S n
no hlh h h hn nt h h h t o h o en l
ne t e h h h t ln n u n
l o n h h l n t n t hn l h
t o en et t n e nlo hu h
T n t hn h



The NSFOCUS ADS solution uses an innovative, multi-stage approach to monitoring, detecting and mitigating the most complex DDoS attacks. All packets are subjected to a series of algorithms to accurately identify malicious traffic. These include Anti-spoofing, Protocol Analysis, Custom Application Analysis, User Behavior Analysis, Dynamic Fingerprint Recognition and Rate Limiting. Together these algorithms provide industry-leading accuracy that protects against both known and zero-day exploits.

The NSFOCUS solution delivered all of the features needed and was the easiest to use and manage. "We found that the other solutions were very complex and required extensive tuning to get the desired result." said Mr. Braunegg. "The NSFOCUS solution just worked. If you plug it in, it will work" he added.



-Logical Deployment

The Results

Since selecting NSFOCUS to protect their network, Micron21 has mitigated thousands of DDoS attacks, substantially improving the reliability of their service offerings. They have also introduced DDoS-as-a-Service to their customers, starting with a single NSFOCUS ADS deployment in North America that has grown to 5 geographically-diverse DDoS clustered scrubbing centers worldwide. This global expansion enabled Micron21 to provide a better service while saving money in the form of reduced bandwidth fees from peering partners. DDoS attacks originate from all over the world, so filtering malicious traffic as close to the source as possible has allowed Micron21 to reduce the amount of overall attack traffic on their network.

Two recent incidents have underscored how successful the NSFOCUS deployment has been for Micron21. James Braunegg recalled that he received a call from the CTO of one of the largest ISPs in Australia asking for help to mitigate a large DDoS attack being experienced by one of their customers. The ISP did not have an effective Anti-DDoS solution deployed and did not have the time to evaluate and install a new solution. Micron21 was able to mitigate the DDoS attack targeting the ISP's core infrastructure quickly and with minimal effort. In yet another incident, one of Micron21's customers experienced an attack that would have brought them down without the use of the NSFOCUS ADS solution. The attack started relatively small, then rapidly increased over the course of 30 minutes. It eventually consumed a staggering 23 Terabytes of inbound data in only two hours, before the assailant(s) ceased the DDoS attack. The peak was 90 Gbps of attack traffic. Given the sheer scale of the problem, a full-blown outage would have potentially cost the end-customer the equivalent of at least $1.3 Million.

Mr. Braunegg has noted that in these instances and more that the "NSFOCUS solution has performed flawlessly

-inside Micron21

NSFOCUS

2.09 Saunders House
52-53 The Mall
London, W5 3TA, UK
Phone:
+44 (0)20 30786850
www.nsfocusglobal.com