#1 November 2019

ENCRYPTED TRAFFIC VISIBILITY

TECHNOLOGY ANNOUNCEMENT: PRE-EMPTIVE DNS SCORING AND BEACONING DETECTION

Helping you protect your business from threats embedded in seemingly harmless batches of emails, such as are used for software updates, and from attackers using fraudulent addresses.

BEACONING DETECTION

Beaconing, which is often used for essentials like software updates or intelligence sharing, can be described as a method for sending/receiving similar sized packets at regular intervals. Command and control servers often use the same methodology to hide from detection.

This new addition to the Barac platform relies on micro segmentation algorithms that have undergone rigorous testing. It detects services that are hogging your bandwidth, and protects against command and control servers and abnormal activity.

Beaconing Detection can be customised to suit your organisation and, like other services on the Barac platform, it operates in real time.

Around 90% of today's data traffic is encrypted

60% of cyber threats are now hidden inside encrypted traffic flows

PRE-EMPTIVE DNS SCORING

Spoofed DNS signatures are used in Phishing attacks and APTs (Advanced Persistent Threats). Until now, protection has relied upon blocking the 'known-bad' contained in a black list of malicious DNS. So G00gle (with two zeros) is unlikely to get through. However, to find its way on to a black list a DNS will have already been found to have caused something bad.

Barac's new Pre-emptive DNS Scoring uses machine learning and supervised classification algorithms to spot bad DNS signatures before anything bad actually happens.

And, because it's what we do best, we analyse the DNS signatures of encrypted traffic.

"The value of your current cyber defences are decreased significantly through data blindness"

– Gartner

Rise Building, 41 Luke Street,
London EC2A 4DP

+44 7555 684 074

barac.io