ENCRYPTED TRAFFIC VISIBILITY

CASE STUDY: BARAC PREVENTS NORTH KOREAN APT HACK

In May 2019 the cyber security team at Barac identified an Advanced Persistant Threat (APT) targeting a global financial institution. The APT was using very advanced encryption to evade detection.

THE ATTACK IN DETAIL

This was a very sophisticated and clever attack. It used encryption and adopted common traffic patterns and profiles to mask its action. The victim was a leading financial institution, with several subsidiaries across Southern Africa.

The institution's security controls dictated that all traffic exiting the business needed to be encrypted. The attackers understood this and used the same approach, hiding the Command and Control (C+C) traffic within encrypted traffic flows so everything appeared normal. The attackers also used a number of fake (spoofed/mangled) websites in Bulgaria for the C+C structure. This meant that the traffic flows appeared to be directed to legitimate sites.

Nevertheless, the Barac Encrypted Traffic Visibility platform flagged these sessions as risky. The platform looks at 200+ metrics – taking into account how these metrics interact over time, in order to create an accurate risk score for the encrypted traffic flows. Using this approach, it identifies small, often easy-to-miss, anomalies in encrypted traffic metadata that can signal a sophisticated threat.

Around 90% of today's data traffic is encrypted

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

Here are some of the metrics, identified by barac, that showed the encrypted traffic leaving the bank's infrastructure was high-risk:

- The Domain Name Server (DNS) risk score was high because its name appeared to have been spoofed.
- There was also a problem with the DNS registry; while it was registered in Bulgaria, the certificates were signed in North Korea.
- The sessions were open for exactly the same duration and the levels of outgoing/incoming traffic were unusually high; these characteristics can be an indicator of a C+C call home message and the exfiltration of data.
- The attack always used the same moderate ciphers, which were not common in the normal traffic flows.

The reason Barac found this highly sophisticated attack was due to our understanding of normal traffic flows, which enabled us to highlight traffic flows outside this norm. This may sound simple, but in fact we use over 200 different metrics and compare their interactions and changes relative to each other over time to be able to detect these kind of attacks.

Rise Building, 41 Luke Street,
London EC2A 4DP

+44 7555 684 074

barac.io