Barac – Encrypted Traffic Visibility

TLS 1.3

KEY BENEFITS

Gain visibility into encrypted traffic.
Expose hidden threats without decryption.
Compliant with TLS 1.3

Maximize security investment.
Optimize performance with efficient management of inbound and outbound encrypted traffic.

Improve risk management and privacy.
Risk reduction though cryptograph compliance monitoring.
Seeing threats and abnormal traffic.
NO decryption means no privacy issues.

Many enterprises have security appliances that seek to look into secured TLS connections to make sure that the enterprise security is appropriately maintained. Whilst this sounds like a magic box that can 'break' encryption, it's not. These systems only work because the certificates that secure the communications have been loaded on to them, and they are also working as their own certificate authorities for the enterprise clients. This also increases the enterprises certificate management overhead.Generally, these appliances utilize whitelists to protect staff privacy these whitelists will include healthcare, banking and other services that hold sensitive personal data. The whitelists are used because staff privacy outweighs the security risk, the appliance will also drop out of proxying connections when they determine the risk is low. Lots of regulatory regimes make it a requirement for regulated industries to inspect traffic as it leaves their network.

WHY SHOULD I CARE?

The IETF published a new version 1.3 of the TLS specification. Version 1.3 addresses a number of deficiencies in TLS 1.2 and things to make the protocol fit for the future:

- TLS 1.3 detects if there is a decryption Man in the middle and will stop the connection
- TLS 1.3 proxying will no longer work, if the appliance drops out of proxying the whole session needs to be restarted (full handshake onwards)
- Certificate information are now encrypted and so cannot be verified. This reduces the efficiency of the current solutions

Challenge

Business is being driven towards encryption by the adoption of Cloud and cloud offerings such as O365, Google and social media are all encrypted, in fact Facebook is already using TLS1.3. The primary driver for encryption is around privacy, with over 80% of page loads now encrypted with SSL/TLS. This growth in encryption presents a challenge: as bad actors now commonly hide threats within encrypted payloads and use encrypted channels to evade detection during data exfiltration. Most organisations lack the tools or are facing challenges associated with SSL/TLS traffic decryption:

- Organizational: Decrypting HTTPS creates privacy challenges for monitored employees. Local regulations or enterprise culture might hinder the decryption project or create internal tensions.

- Technical: The use of decryption architecture degrades the user experience, introducing poor performance and unexpected blocking of legitimate business applications.
- Budgetary: The average cost per user of network security controls will increase dramatically because of the decryption costs, but the overall organizational perception of value might be low
- TLS 1.3: With the emergence of TLS 1.3, decryption will no longer be possible with the session dropped automatically if detecting a Man in the Middle Schema

The Traditional methods are failing

With the impending implantation of TLS 1.3, the only potential decryption methods is to fully proxy all conversations, but with the increase in encrypted traffic this then becomes a major bottle neck and will lead to performance issues as more decryption will mean more machine overhead, leading to higher latency. NSS labs reports show a 672% Response time increase and 60% drop in average throughput when using decryption and service chaining. This does not even touch on the problems caused as crypto keys increase in size. Not to mention the headache of certificate management.

Solution

The Barac ETV platform provides high-performance visibility of inbound and outbound SSL/TLS traffic without the need for decryption, using TLS/SSL Metadata combined with machine learning and behavioural analytics to expose threats and stop attacks. The output of this analysis can be feed into SIEM or SOC implementation to allow the automated analysis of threats. This approach can detect attacks and abnormality on TLS 1.3 without the need for decryption.

How it Works

The Barac Encrypted Traffic Visibility (ETV) platform uses meta data to score encrypted traffic flows. All the Handshake metadata are collected from both the client and the server, sessionized to rebuild the connection and calculate more than 200 indicators that we use to detect correlation of know attacks using machine learning and unknown attacks using behavioural analytics. Those indicators are used to create unique signatures for the encrypted traffic allowing to detect any changes or malware indicators instantly.

The Barac collectors take traffic from a Span or mirror port, the meta data is then sent securely to the Barac ETV platform where analysis is run, this allows for fingerprinting of know attacks and machine learning of the normal traffic flows allowing the flagging of ab normal traffic. The alerts are sent to the main platform and to the SIEM or SOC platform

Unique

Barac is able to analyse TLS 1.3 traffic in real time without decrypting it

The Answer

By looking at the meta data of the packets Barac is really the only solution that provides visibilty of threats at scale whitlst maintaining privacy.

Contact:
sales@barac.io