ENEA

PRESS RELEASE

Enea Announces New Smart Tools to Identify Encrypted and Evasive Network Traffic

The Enea Qosmos ixEngine delivers the traffic visibility that solution vendors need to optimize network security and performance, while safeguarding privacy

STOCKHOLM, Sweden, February 12, 2020 – Enea® (NASDAQ Stockholm: ENEA), a global supplier of innovative software components for cybersecurity and telecommunications, is pleased to announce enhancements to the Enea Qosmos ixEngine® and Enea Qosmos Probe products that deliver greater insight into encrypted and evasive traffic.

Anonymity and privacy technologies, like data encryption and VPNs, are vital for safe and secure communications, but they limit the visibility network professionals rely on for troubleshooting, performance optimization, and business analytics. They also impact cyber security specialists, who need traffic visibility to detect and analyze threats in networks.

Providers of network management and security products have long relied on Enea's Qosmos traffic intelligence technology for exceptional visibility and rich data sets that enable them to differentiate their products in continuously evolving markets. The rise of encrypted and evasive traffic may be a challenging evolution, but as with others that have preceded it, Enea can help its customers transform change into competitive advantage.

To this end, the company has created a special team dedicated to developing innovative techniques for extracting maximum insights from encrypted and evasive traffic, while packet content remains private. The efforts have resulted in recent product enhancements that deliver unique visibility of 6 types of evasive traffic:
- Cryptocurrencies and mining pools
- Covert communication channels
- VPNs (Virtual Private Networks)
- Anonymizer applications
- Traffic spoofing applications
- Embedded links in emails

"As the use of encryption increases - and becomes more robust with TLS 1.3 - and as evasive tactics become more complex, innovation is key for our customers to maintain the critical visibility they need to optimize performance and respond to threats," said Jean-Philippe Lion, Senior Vice President of the DPI Business Unit at Enea. "With our new and enhanced capabilities, we are confident our clients will be able to meet the challenges of encrypted and evasive traffic head on, and develop even stronger and smarter solutions for protecting networks."

The enhanced versions of the Enea Qosmos ixEngine and Enea Qosmos Probe products will be presented at the Enea booth (#236) in the South Expo hall at RSA Conference 2020. For more details or free expo passes, go to https://www.qosmos.com/rsa-conference-2020/. Personal demonstrations during the event can be requested by sending an email to rsa@qosmos.com.

Additional Resources

For additional information about encrypted and evasive traffic, visit our dedicated resource hub at https://www.qosmos.com/resources/use-case-hubs/encryption-2/.

To learn more about Qosmos traffic classification, explore the Qosmos Labs Protobook at https://protobook.qosmos.com/index.html/.

Details of the product enhancements:

- **Cryptocurrencies and Mining Pools**
  A dozen of the cryptocurrencies and mining pools most commonly involved in cyberjacking, data exfiltration, and other cyberattacks have been added to Qosmos ixEngine, including Ethereum, Monero mining pools, and Ripple.

- **Covert Communication Channels**
  New capabilities have been added to detect non-standard tunneling activities over legitimate protocols, such as DNS (Domain Name System) and the ICMP protocol (Internet Control Message Protocol), which may indicate unauthorized or illegal activities.

- **VPNs (Virtual Private Networks)**
  Identification and classification of over a dozen new VPNs have been added, including TunnelGuru, Hexatech, and Windscribe VPN. In total, Qosmos ixEngine now supports more than 80 VPN and tunneling-related protocols. The processing analytics include identification of mechanisms which might indicate the cloaking of unauthorized or illegal activities.

- **Anonymizer Applications**
  Enea has added classification of four new anonymizer applications to Qosmos ixEngine, bringing the total to two dozen, including anonymizers which encapsulate communications in multiple layers of encryption.

- **Traffic Spoofing Applications**
  Classification has been extended to additional traffic spoofing applications (like eProxy, and HTTP Injector) that seek to deceive conventional packet inspection technologies by employing multiple evasive techniques (e.g., protocol header customization, proxy servers, tunneling and domain fronting).

- **Embedded Links in Email**
  Recent product enhancements also include the extraction of URLs (web links) from emails sent using SMTP, POP3, and IMAP protocols. This data offers an important complement to anti-virus tools that seek to identify and block malicious code cloaked in seemingly innocuous email communications.

These recent enhancements complement the existing capabilities of Qosmos ixEngine to deliver visibility into traffic using other evasive techniques including:

- **Encryption:** Maximum visibility into all encrypted traffic to support triage for decryption, advanced analytics for anomaly detection, and forensics.
- **Complex Tunneling**: Deep visibility into traffic using complex tunneling, with full protocol paths revealed for up to 16 levels of encapsulation.
- **Domain Fronting:** Exposure of routing schemes in Content Delivery Networks (CDNs) and other services that mask the intended destination of HTTPS traffic (direct or tunneled).
- **File Spoofing:** Detection of inconsistencies such as a false MIME type or a mismatch between the original hash and the computed hash**.**

Media Contact
Erik Larsson, SVP Marketing & Communication, Enea
Phone: +46 8 507 140 00
E-mail: erik.larsson@enea.com

About Enea
Enea is a world-leading supplier of innovative software components for telecommunications and cybersecurity. Focus areas are cloud-native, 5G-ready products for mobile core, network virtualization, and traffic intelligence. More than 3 billion people rely on Enea technologies in their daily lives. Enea is listed on Nasdaq Stockholm. For more information: www.enea.com