ROHDE&SCHWARZ
Cybersecurity

press RELEASE

DNS Tunneling Detection Feature of Rohde & Schwarz Cybersecurity's Network Traffic Analysis Software Eliminates Weak Spots of Firewalls to Preserve Security

The OEM deep packet inspection software R&S PACE 2 now improves the reliability and credibility of network protection solutions. When embedded in a firewall, malicious attacks that bypass common security policies via DNS tunneling can be identified and prevented.

Leipzig, Germany – August 28, 2017 – Rohde & Schwarz Cybersecurity, a leading IT security company, today announced the launch of enhanced traffic analysis capabilities to detect DNS (Domain Name Server) tunneling. The new functionality provided by the deep packet inspection (DPI) engine R&S PACE 2 can be utilized by IT security solutions to reliably detect malicious activity in network traffic in real time caused by DNS tunneling.

DNS is a core component of the Internet and of paramount importance to the operation of the World Wide Web. It provides the mapping service between a domain name and the corresponding IP, translating human-friendly domain names into IP addresses.

As DNS is a trusted protocol it is often overlooked for security as no one considers using the protocol for data transmission. The use of DNS, especially with port 53, for data theft is called DNS tunneling. In tunneling, cybercriminals use the DNS protocol as an established pathway to direct the exchange of information for malicious purposes. Several tools have been developed to bypass traditional IPS or firewall inspection and network security measures to reach the Internet.

With the enhanced DNS tunneling detection functionality of the DPI engine R&S PACE 2, Rohde & Schwarz Cybersecurity now provides a highly scalable OEM software solution for network protection products. When embedded in a firewall, IT security vendors are able to inspect the entire DNS query for deeper markers of either good or bad behavior. This way, malicious attacks that bypass common security policies via DNS tunneling can be identified and prevented.

According to the DNS Threat Survey 2017 by Efficient IP, 94 percent claim DNS security is critical for their business. This is not surprising as in the past year, 76 percent of organizations around the world have been subjected to a DNS attack and a third suffered data theft. In addition, DNS tunneling was one of the leading causes besides malware, DDoS and cache poisoning attacks. If not secured properly, DNS attacks could cost businesses over $2 Billion annually in data exfiltration, loss of business or application downtime, says EfficientIP.

The new DNS protocol classification feature not only adds further value to cybersecurity solutions but also improves their reliability and credibility that enterprises can rely on.

Besides the ability to detect DNS tunneling, R&S PACE 2 also provides reliable detection of tunneling in the HTTP protocol.

The DPI software library R&S PACE 2 provides powerful and reliable detection and classification of thousands of applications and protocols by combining deep packet inspection and behavioral traffic analysis – regardless of whether the protocols use advanced obfuscation, port-hopping techniques or encryption. DPI is needed everywhere in the network where intelligent decisions need to be made based on the nature of IP traffic, whether it is wanted or unwanted traffic, good or malicious.

Press Contact:

Christine Lorenz, Phone: +49 34159403062, Email: christine.lorenz@rohde-schwarz.com

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity is a leading IT security company that protects companies and public institutions around the world against cyberattacks. The company develops and produces technologically leading solutions for information and network security, including highly secure encryption solutions, next generation firewalls and software for network analysis and endpoint security. The award-winning and certified IT security solutions range from compact, all-in-one products to customized solutions for critical infrastructures. The product portfolio also includes vulnerability scanners and firewalls for business-critical web applications. To prevent cyberattacks proactively, rather than reactively, our trusted IT solutions are developed following the security-by-design approach. More than 500 people are employed at the current locations in Germany, France and Denmark.

Rohde & Schwarz

The Rohde & Schwarz technologies group offers innovative solutions in all fields of wireless communications as well as in IT security. Founded more than 80 years ago, the independent company has an extensive sales and service network with subsidiaries and representatives in more than 70 countries. On June 30, 2016, Rohde & Schwarz had approximately 10,000 employees. The group achieved a net revenue of approximately EUR 1.92 billion in the 2015/2016 fiscal year (July to June). The company is headquartered in Munich, Germany, and also has strong regional hubs in Asia and the USA.