

Inbjudan till Live meeting-webinar

NetWitness Spectrum

“Automated and Absolute Identification of Zero-Day and Targeted Malware.”

Tisdagen den 18 oktober, 2011

14.00–15.00 CET



NetWitness Spectrum™

Absolute Identification of Zero-Day and Targeted Malware

Is your organisation vulnerable for Zero-Day and Targeted malware?

Join NetWitness and Rebendo to learn how to achieve Automated and Absolute identification of Zero-Day and Targeted Malware attacks. Zero-day and targeted malware is successfully compromising your network and evading existing security technologies. Why? Modern malware is designed to behave like legitimate traffic and communicate undetected. NetWitness developed Spectrum in response to demand from security professionals for precise and pervasive identification and prioritization of the broad range malware-related threat.

What Attendees will learn:

- How to achieve Automated and Absolute identification of Zero-Day and Targeted Malware attacks
- Options to improve your organisations Information Risk Management strategy.
- How to improve your organisation’s ability to proactively protect your Intellectual Property
- How modern malware can infect your IT systems

Who should attend:

- Chief Information Security Officers
- Information security professionals
- Security Project Managers
- Networking & Telecommunication professionals



Presenter:

Anders Svensson,

RSA/NetWitness, Information Security specialist



Moderator:

Anders Eriksson

Rebendo, Oversees the new commercial activities at Rebendo Konsult AB. Anders has a long track record within the IT, Broadband, Data and Telecommunications industry.

NetWitness® is a revolutionary network monitoring platform that provides enterprises a precise and actionable understanding of everything happening on the network. NetWitness solutions are deployed in customer environments to solve a wide range of challenging information security problems including: insider threats, zero-day exploits and targeted malware, advanced persistent threats, fraud, espionage, data leakage, and continuous monitoring of security controls.

The Need for A New Approach

Over the past several years, advanced and zero-day malware attacks have become a growing problem with no sign of abatement. This issue has become the top concern for most security organizations. Nearly every investigated case of data leakage, financial loss, or other network breach involves some form of malicious executable (i.e., customizable commercial malware or custom malicious code) that is being used to maintain a foothold into compromised networks. Obfuscation techniques are evolving at an increasing rate and traditional security tools cannot consistently keep up. The current threat environment demands a new, agile approach to the detection of malware.

NetWitness Spectrum – A Revolutionary Approach

Spectrum is built upon the award winning NetWitness network monitoring platform, which provides enterprise-wide visibility and complete knowledge of all network activity. In addition to utilizing this unparalleled visibility to identify executable content wherever it exists, Spectrum is able to answer any question about the related behavior of that executable in the context of the unique environment that is your organization’s network. In effect, Spectrum is able to consider the history of your entire network’s interaction with each threat actor on the Internet, and adjust the levels of scrutiny accordingly. It’s like having an HD video camera attached to every object crossing the wire.

For each piece of executable content found on the network, Spectrum will ask thousands of questions concerning the file. At a high level, Spectrum:

- Mimics the techniques of leading malware analysts by asking thousands of questions about an object and all of its related network behavior, without requiring a signature or a known “bad” action.
- Leverages NetWitness Live by fusing and triangulating information from leading threat intelligence and reputation services to assess, score, and prioritize risks.
- Utilizes NetWitness NextGen’s pervasive network monitoring capability for full network visibility and extraction of all content — executable and metadata — across all protocols and applications.
- Provides transparency and efficiency to malware analytic processes by delivering complete answers to security professionals, including a wealth of detailed supporting data, such as: intelligence fusion, sandboxing, correlation, and scoring options that are designed for diverse environments and rapidly evolving threats.

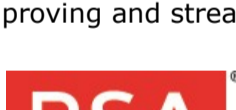
When combining these distinct analytic and scoring methods with the unique benefits obtained from pervasive visibility into content and behavior, NetWitness Spectrum provides an unmatched capability to detect and identify zero-day malware.

Spectrum offers the first analytical workflow combined with a complete rendering of network traffic for ubiquitous, automated malware analysis; thus, delivering the most comprehensive identification, investigation and risk-based prioritization of malicious content activity directly into the hands of security teams. Security operations teams can effectively and efficiently determine proactive remediation efforts based on the solution’s results.



NetWitness will become a core element of RSA’s Advanced Security Management Solutions, providing real-time visibility into network activity and adding efficiency to incident investigations and workflow. By combining the NetWitness network monitoring and analysis technology with RSA’s enVision® platform, RSA® Data Loss Prevention Suite (DLP) and RSA® CyberCrime Intelligence service, security teams can achieve deep insight into the security posture of their organizations. The precise intelligence and visibility that NetWitness provides, coupled with the RSA Archer eGRC platform, enables organizations to apply business context to security information for better identification and prioritization of security risks while improving and streamlining the incident management process.

www.netwitness.com



RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com



Rebendo är ett svenskt konsultföretag med en produkt- och tjänstportfölj som maximerar, kvalitetssäkrar och mäter prestandan i de centrala IT-systemen. Rebendo startade sin verksamhet 2001 och huvudkontoret ligger i Stockholm, Gröndal.

Vår affärsidé är att säkerställa maximal tillgänglighet och effektivitet i IT- och telefoniverksamheten på företag, organisationer och offentlig sektor. Rebendo är svenska representanter för Netwitness.

www.rebendo.se

Registration:

Yes I/We register for the above webinar **Automated and Absolute Identification of Zero-Day and Targeted Malware, October 18 2011 at 14.00 –15.00 CET**

Name E-mail.....

Dept Phone.....

Name E-mail.....

Dept Phone.....

Company/Org.....

Address.....

ZIP.....City

Send the above registration data to: anders.eriksson@rebendo.se or call Anders Eriksson, Rebendo Konsult AB +46 8 681 15 59, **before Oct 17, 2011**

Time and place:
October 18 2011, 14.00 –15.00 . Login data to the webinar will be sent after registration.

The webinar is free.



Ormsbergsvägen 4
117 67 STOCKHOLM
Telefon: +46 8 681 15 50
Fax: +46 8 681 15 56
E-post: info@rebendo.se
www.rebendo.se



Automated Malware Analysis

Absolute identification of zero-day and targeted malware