Symantec Technology Integration Partner: TopSpin Security

Business Challenge

SSL/TLS encrypted traffic is pervasive in organizations around the world, representing over 35% of all enterprise network traffic today. With a 20% annual growth rate, SSL/TLS encrypted traffic increasingly presents a blind spot in organizations; most current security solutions cannot see or manage this traffic, making it harder to identify and control malicious activity coming into and leaving enterprise networks – especially malware communication with command and control systems.

Solution: Symantec and DECOYnet™

Symantec's Encrypted Traffic Management solutions eliminate the encrypted traffic blind spot and combat the security threats hidden in encrypted traffic. Using Symantec inspection and decryption technologies like Symantec SSL Visibility, DECOYnet is able to run its analysis engines on a network to identify all malware activities as well as automatic, potentially hidden, communication channels.

DECOYnet has been designed to address the very characteristics that prevent current solutions from successfully identifying infected assets in a short timeframe. It provides a combination of incident reporting accuracy, appropriate forensic information, filtering out all but the most high-risk traffic, visual analytical tools, rapid deployment and automated maintenance. Throughout the monitoring, an ongoing automated process is analyzing all the protocols involved in the traffic flow, starting with TCP, DNS, SSL, HTTP, FTP, SSH, etc. and using its patent-pending technology to identify the Human Browsing Session traffic. These different events are correlated over time to produce accurate incident reports equipped with all the required forensic data supporting quick identification of the attacker's activities.

Symantec SSL Visibility is an integral component to an organization's encrypted management strategy. This innovative appliance identifies, inspects and decrypts multiple streams of SSL/TLS network traffic across all network ports to provide security devices with the necessary visibility and control of previously encrypted traffic and applications. SSL Visibility identifies all SSL traffic regardless of TCP port or application and allows the control of this traffic via advanced policies. By selectively decrypting traffic, organizations can effectively control and balance the data privacy and compliance requirements with the necessary security to protect them against modern threats.

By combining SSL Visibility with TopSpin's DECOYnet, you can now analyze network traffic of all kinds and in all parts of the network, including encrypted traffic, to best detect and defeat attacks in progress. DECOYnet reveals the presence of malware and attackers that have infiltrated your network to steal your information, using a new and unique approach of decoys and traps in the network, while identifying CnC-asset communication. Once DECOYnet has discovered an attacker at work, it proceeds to deceive, confuse and slow down the attack. This is a very different mode of operation compared to security products such as firewalls, IPSs and anti-virus, which attempt to identify and stop malware from entering your system. DECOYnet by comparison is dedicated to identifying intruders by their behavior without any preconceptions about how the target suspect might look,

Partner: TopSpin Security

Partner Product: DECOYnet™

Symantec Product: SSL Visibility

or how it came to be there. DECOYnet is easily installed out of line in the network requiring minimal configuration. Incidents are quickly analyzed by the security team based on the precise information provided for each one of the correlated events.

How it Works

The diagram below demonstrates how Symantec and TopSpin work together to provide a more effective defense-in-depth solution for advanced threats.

SSL Visibility uses its comprehensive policy engine to selectively decrypt traffic and send it to the TopSpin DECOYnet devices, which then run their analysis engines to identify and detect all malware activities in the network.

Benefits

The combined SSL Visibility and TopSpin Security solution:

- Comprehensive network visibility into all traffic, encrypted or otherwise

- Powerful policy-based enforcement of inbound and outbound traffic

- Apply all analysis engines for the entire egress/ingress traffic

- Detect the malware whether it is using plain text or SSL/TLS

- Detect all communication channels used by the organization
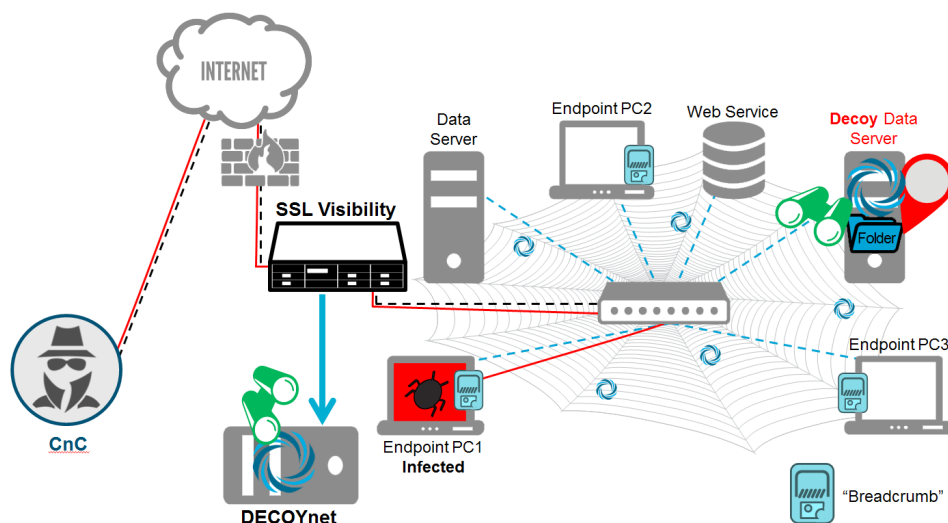
About TopSpin Security

TopSpin Security provides a solution that protects your organization from loss of valuable data and prevents disruption of your operations. The emphasis is on accuracy, minimal overhead and simplicity of deployment and usage. The company's solution DECOYnet™ incorporates a set of unique security engines that discover infected assets in your organization before damage is done. These include active deception, automatic configuration to your network and automated structured analysis of your network traffic.

Learn more: www.topspinsec.com, our blog and Twitter.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com