BIZCOMMUNITY

Check Point's 100% catch rate in benchmark test

Check Point Threat Prevention has achieved a 100% catch rate of unknown malicious files in recent benchmark testing. 300 unknown malicious files were scanned through a Check Point 13500 security gateway running ThreatCloud, and through competitive products from three other security vendors.

Check Point
SOFTWARE TECHNOLOGIES LTD.

All platforms used in the test were activated with the maximum number of threat prevention services (IPS, anti-malware, anti-bot, Threat Emulation) and with the most up-to-date signatures. The results showed that Check Point outperformed all the other solutions, with an unknown malicious file catch rate of 100%. The second-ranked competitor recorded a catch rate of 70%. The 300 malicious files were a mix of 40% pdf files, 40% exe files and 20% doc files.

As the modern threat landscape evolves with more aggressive and destructive generations of targeted attacks, Check Point solutions have accelerated detection and increased awareness of these new, emerging threats. Check Point's global research in its 2014 Security Report found that on average, an organisation downloads 53 unknown malware agents per day - or one every 27 minutes.

Zero-day attacks 144% up

"Hackers are going to ever-greater lengths to find and exploit newly discovered vulnerabilities, investing significant resources into developing new malware variants and attack vectors to infiltrate a network. Our research shows that since 2012 zero-day attacks have increased by 144%, which highlights the rate at which organisations are facing advanced and unknown attacks," said Doros Hadjizenonos, Check Point South Africa's Sales Manager. "With a catch rate of 100% of unknown malicious files, our Threat Prevention technologies give our customers the highest levels of protection against undiscovered malware in the industry's most comprehensive multi-layered security solution."

An integral part of Check Point's multi-layered Threat Prevention, Threat Emulation discovers and prevents infections from undiscovered exploits, unknown variants of malware, and targeted attacks by dynamically emulating files within a virtual sandbox. Threat Emulation provides updates on and blocks latest attacks in real time, while its closest performing competitors detect unknown malware but cannot prevent it from entering the network: they allow all files into the network while the suspicious files are being uploaded and emulated, with a delay of 30 minutes or more before updated signatures

are created to block the unknown malware. This timeframe allows a significant window for malware propagation in the network.

Once identified, Check Point researchers immediately evaluate the behaviours and properties of these unknown threats and quickly develop protections. These protections are automatically distributed across all Check Point gateways globally utilising ThreatCloud. ThreatCloud is Check Point's collaborative threat intelligence network, which provides for automatic, real-time protection to the company's worldwide customers. During the 'Unknown 300' benchmark testing, Check Point was the only solution that offered detection and prevention with competitors only demonstrating the ability to detect new threats and attacks.

The full report is available from www.checkpoint.com/campaigns/300/300TestReport.pdf