HealthManagement
Promoting Management and Leadership

Prevention is the Best Form of Medicine

Greg Maudsley
******@***menlosecurity.com

Senior Director, Product Marketing
- Menlo Security
California, U.S.

Hospitals and other healthcare organisations (HCOs) are increasingly singled out by cyber criminals for ransomware and other attacks. Not only are patients' sensitive records being targeted, but also their intellectual property or credit card information. The primary reasons for the HCO vulnerabilities are outdated security architectures, and overall lack of IT security experts. Isolation technology provides an appealing alternative to traditional security methods, and prevents, rather than treats, malware and phishing attacks, explains Greg Maudsley, a cyber security expert for Menlo Security

Why are HCOs Susceptible?

Today's targeted attacks are mostly motivated by financial gain rather than notoriety. Cybercriminals target organizations with the weakest defenses and most valuable data – and few industries are as data-dependent as healthcare.

Without patient records, a hospital is powerless. Staff routinely access critical information from multiple, often unsecured, devices or networks. This rules out perimeter-based security, while the spread of network ingress and egress points – and so attack vectors – make hospitals a soft target. Tight budgets and other priorities mean that hospitals typically lack specialist IT security skills and experience, they fail to conduct regular security audits and are in an endless game of "catch-up".

The Doctor Has Become Patient Zero

"Patient Zero" describes the first human infected by a new or recently discovered viral or bacterial outbreak. In IT security it means the first individual to be infected by a new malware strain, or a first phishing victim. Patient Zero comes into contact with others and the infection spreads exponentially, until experts cure the disease or limit its propagation. Even with today's science, this can take months or years – and millions can suffer.

The same applies to IT infection – although many like to believe that state-of-the-art security solutions should immediately respond and eliminate the threat. Today's security solutions rely on recognizing good versus bad. We may have a solid grasp of what is good and bad today, but no way of knowing what will be good or bad tomorrow. Even with machine learning and Artificial Intelligence, there can be days, weeks, or months between "patient zero" infection and effective mitigation – leaving hundreds or thousands of infected devices. We will never be able to anticipate every new malicious web link or malware exploit: so prevention holds the key.

A Preventative Approach

Isolation offers a new approach to this challenge. It implements a secure and trustworthy execution environment (or isolation platform) between the user and potential sources of attack. Executing sessions separated from the end device, and only delivering safely rendered material to that device, mean that users are protected from malware and phishing attacks. While legitimate content is faithfully rendered, malware has no path to reach the endpoint. So administrators can safely allow users greater Internet access, while eliminating the risk of attack.

Healing Qualities

With the right isolation technology, HCOs can heal their IT security weaknesses, and reap a number of benefits over legacy security products:

Firstly, isolation is 100 percent effective in preventing malware from web and email links. User sessions are executed in virtual containers within the isolation platform. Each time a user completes a session, all content, including any malware, is automatically erased along with its container, leaving no chance for malware to escape and infect the endpoint. This means no false positives to block legitimate content and generate alerts, and no false negatives that allow malware to reach its target.

Secondly, the user experience is indistinguishable from browsing the web directly. There is no noticeable latency during browser operations, no pixilation, choppy scrolling or other visual artifacts common with ‘screen-scraping’ technologies like VDI. Isolation uses the optimal encoding mechanism for each type of content, and delivers it securely to the user’s device using industry-standard rendering elements compatible with any device, browser or operating system.

Thirdly, cloud-based isolation deploys quickly and easily and reduces security complexity and costs because it needs no extra endpoint hardware or software. It can be turned on in minutes and simplifies operations by eliminating “alert fatigue” from false positives and negatives. It also scales to the demands from small to global HCOs.

Finally, isolation can be used in conjunction with existing security infrastructure. Next generation firewalls, for example, which protect against the latest cyberattacks, become even more versatile and effective when integrated with threat isolation.

It’s Time for HCOs to Become Immune to Malware and Phishing

Cybercriminals will always target those organizations with the weakest defenses and the most valuable data. Hospitals will inevitably possess the most valuable data, but by bolstering their cyber immunity with the latest technology, they can make themselves a far less tempting target for ransomware and other cyber threats.

Published on : Tue, 18 Apr 2017