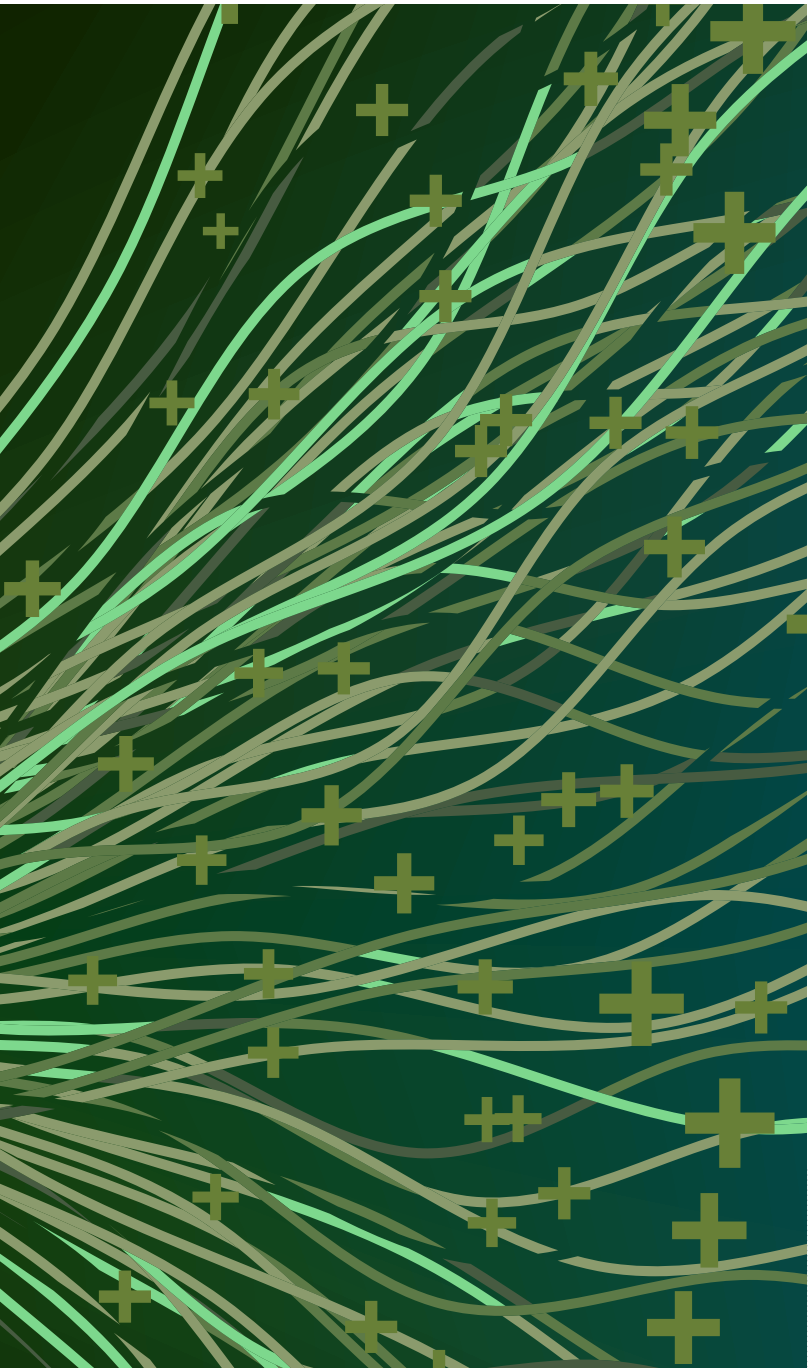
SearchSecurity

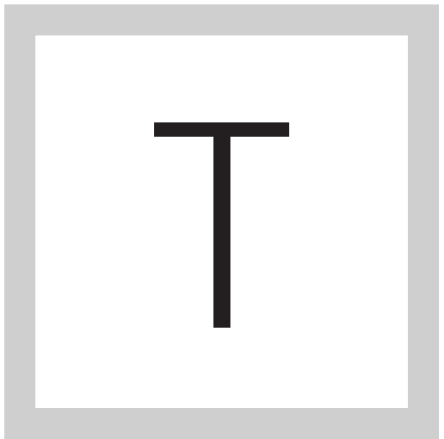


E-Guide

WEB BROWSER SECURITY FEATURES MAKE ATTACKS HARDER

TechTarget

SearchSecurity



HIS EXPERT E-GUIDE will showcase the analysis and hacking contests that illustrate browser security improvements for your organization.

SearchSecurity

WEB BROWSER SECURITY FEATURES MAKE ATTACKS HARDER

Security capabilities built into popular browsers are making it more difficult than ever for cybercriminals to carry out attacks using browser vulnerabilities, according to security experts. While the security improvements don't make browsers bulletproof, recent hacking contests demonstrate the overall enhanced state of browser security.

Microsoft, Mozilla and Google have all been developing support for substantial security capabilities in recent years that isolate critical components and help prevent attackers from using the browser as a stepping stone to a more substantial attack, says Chris Valasek, senior research scientist at Accuvant Labs.

"It's accepted that users will click on links and browsers will be exploited, but if you have something to contain the attack you are going to be much better off," Valasek says. "As long as there are smart attackers out there with time on their hands they're going to take vulnerabilities and create something to exploit them, but we're seeing that it's taking more time and more effort."

At RSA Conference 2012, Valasek and his team, which includes researchers Joshua Drake and Paul Mehta, talked about Web browser security features and the results of their browser security analysis of Mozilla Firefox, Microsoft Internet Explorer and Google Chrome. The analysis found all three browsers contain capabilities that make an attacker's job much harder. The Accuvant Labs researchers praised Google's implementation of sandboxing in Chrome for making it an extremely difficult browser to crack. Sandbox technology – also implemented in Internet Explorer – is intended to contain certain actions, such as code execution.

"While not perfect, sandboxes do provide a huge barrier of entry of any persistence on anyone's machine," Valasek says. "It might make an attacker look for lower hanging fruit."

Both IE and Chrome also support JIT hardening, a function that reduces the impact of vulnerabilities in other software. The browser JIT engine is among the favorite targets of attackers.

All three browsers use address space layout randomization (ASLR) and data execution prevention (DEP), technologies designed to prevent an attacker from using well-known locations to begin exploitation and from exploiting code in certain regions of memory. The browsers also contain a stack cookies

function, which is designed to prevent stack-based buffer overflows, a common component to a successful attack.

"We can beat up on Firefox or Internet Explorer and even Chrome, but all of these browsers improved drastically since where they were at four years ago," Drake says.

However, as with any security technology, there is no silver bullet, he adds. All of the security features contain weaknesses that can be exploited by a skilled attacker. Still, the increasingly difficult nature of carrying out an attack targeting the browser vulnerability was put on display in March at the CanSecWest security conference in Vancouver BC, where Google and HP TippingPoint held their annual browser busting contests. While several winners were crowned, the contestants reportedly admitted that it took long hours to string together an attack scenario that enabled them to break out of the browser and onto the machine.

A team of researchers from VUPEN Security strung together multiple vulnerabilities in a complex exploit to garner $60,000 from Google. Other white hat hackers in the contest failed to pull off a complete attack. This year's contest stood in stark contrast to years past when multiple security researchers took mere minutes to demonstrate a vulnerability and compete a successful

browser attack.

For the Pwn2Own contest run by HP's TippingPoint Zero Day Initiative, the research team from VUPEN demonstrated a successful attack against Chrome and Internet Explorer, while independent researchers Vincenzo Iozzo and Willem Pinckaers teamed up to successfully exploit a Firefox zero-day flaw.

Despite the improvements in browser security, spear phishing and other email attacks targeting browser vulnerabilities and browser components like Adobe Flash and other plugins, are almost constant and a serious problem for enterprises says Anup Gosh, founder and chief technology officer of hardened-browser maker Invincea. Gosh, who received funding from DARPA to create a virtual sandbox browser environment that supports Internet Explorer and Firefox, says a lot of organizations are still using outdated browsers with fewer security features to support custom applications.

"When you talk to people who clean up networks and the incident response guys, it's all spear phishing right now," Gosh says. "It's not hard to get a user to click on a link and exploit a browser component vulnerability. The weaknesses are still there."

SearchSecurity

ROBERT WESTERVELT is news director of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com.

SearchSecurity

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.