Protecting against mobile and web security threats

Jezmynn Koh, 2014-10-10

Estimates indicate that 37.3 million Internet users worldwide experienced phishing attacks from May 1, 2012 to April 30, 2013 and 1 million U.S. computers were infected with banking malware in 2013.

Security threats to organisations

Organisations with public-facing web services — particularly banks and financial institutions, e-commerce companies, and social media sites — are increasingly vulnerable to malware and phishing attacks designed to steal identity, data, and money.

Organisations are also facing an escalated vulnerability to web-based malware, which has arisen with the increased use of the corporate network to access web- and cloud-based tools, SaaS applications and social media sites.

Both have been the cause of innumerable security breaches in recent history with organisations of all sizes.

The recent Heartbleed attack exposed all businesses that were running vulnerable versions of the OpenSSL protocol. A closer look at the reported attacks on organisations such as Apple Daily and Paypal explains the consequences and sophistication of these attacks. A distributed denial-of-service (DDoS) attack launched on the Apple Daily site saw 40 million enquiries being sent to the site every second, blocking the site's daily readers for hours. In the case of Paypal, a sophisticated phishing attack was launched after hackers saw redirection vulnerability in the wake of the Heartbleed bug. Even though Paypal had switched to a new SSL certificate, it had not revoked the compromised pre-Heartbleed one. Other high profile attacks, such as the Adobe data breach, attack by The Messiah in Singapore, the recent multi-layer distributed DDoS attacks, SQL injection vulnerabilities, and JSON payload violations in AJAX widgets, pose increasing risks to interactive web applications, data, and the business.

Organisations will find themselves, the consumers and employees at risk if they don't adequately protect their networks, applications, and data. Therefore, these days, a key business challenge is to ensure: firstly, data protection and safety of customers while maintaining an unchanged user experience across web-based and mobile platforms, and secondly, the protection against websites laden with malware that threaten to infect the organisation's network. Multiple consequences may arise if the necessary precautions are not taken.

Asset loss

Many organisations have lost assets amounting to millions of dollars per year. Some banks, which tried to push these costs onto customers, not only suffered financial losses but also public backlash. Repeated breaches have also led to retail brands losing customer confidence in online banking and e-commerce.

Overworked anti-fraud teams

The sheer volume of data and security breaches have also led to in-house anti-fraud teams to become increasingly overwhelmed trying to find a root cause. Most have adopted or are considering the adoption of a multi-layered strategy of deploying multiple technologies in order to plug the gaps.

Infection from web-based threats

Should malware get an opportunity to sneak in and infect systems the network, sensitive data and company trade secrets may be at risk.

How can F5 help?

F5's Web Fraud Protection and Secure Web Gateway (SWG) solutions provide both the breadth and depth of coverage organisations need to gain a full defense against malware, phishing attacks, and asset loss due to fraud.

Edwin Seo, Regional Security Architect, APJ, at F5 Networks says, “Sophisticated attacks like these increasingly cause serious disruptions for organisations. F5 is one of the few security companies worldwide that can offer a broad range of security solutions. This range of solutions provide holistic protection for today’s organisations ranging from security against fraud, web-based malware, DDoS attacks and other threats via web applications.”

F5’s Web Fraud Protection reference architecture comprises F5 MobileSafe™ and F5 WebSafe™. While MobileSafe provides fraud protection for mobile devices and applications, WebSafe enables enterprises to protect their customers from online-based threats such as credentials theft, automated fraudulent transactions, and phishing attacks. This solution is distinct from competitors’ offerings because it is a clientless solution that can transparently inspect the endpoint, detect malware activity, and provide protection from it. It also features year round support provided by F5’s Security Operations Center (SOC). The SOC monitors attacks in real time, notifies customers of threats, and if necessary, can shut down phishing sites.

F5’s SWG helps organisations in the region defend themselves against potential malware encountered by their employees as they access websites, web-based applications, SaaS applications and social media platforms. F5 Secure Web Gateway Services ensures employees access the Internet in ways that enhance their productivity and, at the same time, protects the enterprise from potential liability and web-based threats.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com