Cure Your Big App Attack

Peter Silva, 2011-22-06

Not that I really needed to point his out but, security attacks are moving 'up the stack.' 90% of security investments are focused on network security, yet according to Gartner, 75% of the attacks are focused at the application layer and '*over 90 percent of security vulnerabilities exist at the application layer, not the network layer*.' SQL Injection and XSS are #1 and #2 reported vulnerabilities and the top two from the OWASP Top 10. Plus, from Forrester Consulting, the average loss of revenue per hour for a layer 7 DDoS attack is $220,000. These vulnerabilities are some of the primary routes that are being exploited in many of the recent attacks.

Modern DoS attacks are distributed, diverse and cross the cavity that divides network components from application infrastructure yet many of these attacks are preventable. The problem is that organizations are using outdated network and/or desktop technology to try and protect against sophisticated application security attacks which traditional solutions like network firewalls, IPS or AV systems have little to no visibility or role. It's like trying to protect a city against a coordinated air attack by digging trenches in the ground. Wrong band-aid for the attack vector.

The solution is an integrated approach that covers network and application security along with access control. Another dilemma is that security has often been left up to the network gang who may or may not have expertise in and around the transport and application level exploits. And deploying more network firewalls, AV, or IPS systems is not really the answer. You might just be digging more trenches. F5 has technologies like BIG-IP ASM, APM, Edge Gateway and LTM that can help mitigate the recent attacks. Many of our solutions (particularly ASM) have capabilities to prevent DoS, DDoS, Brute Force, Parameter Tampering (and dynamic parameters), Forceful Browsing, Web Scraping, SlowLoris, Access Control, XSS, SQL Injection and the entire OWASP Top 10. ASM can also be configured to verify the value of web application set parameters isn't changed during the user's session along with ensuring a user has accessed the site via a login page. With those recent attacks, ASM could have blocked or at least alerted site owners of the intrusion. Detecting and alerting on this when it started, even without mitigating would have considerably minimized the business risk. BIG-IP LTM can protect you from a network perspective with BIG-IP ASM from an application angle.

It is interesting that these attacks have been around for a while but also shows how hard it is to get protection right, especially when the attacks are blended. Once a vector is found to deliver, a variety of exploits can be used in quick succession to find one that will work. Most of these attacks would also have sailed invisibly through an IPS device – no offense to those solutions – they are just not designed to protect the application layer or didn't have a signature that matched. A unified application delivery platform with multi-layer visibility is the best way to detect and mitigate multi-layer attacks.

ps

Resources

- Ongoing storm of cyberattacks is preventable, experts say
- With a click, employees invite a vampire into the network
- DataLossDB
- Codemasters email customers regarding recent security breach
- Thieves Found Citigroup Site an Easy Entry
- Sega Is the Latest Victim, Admits User Accounts Hacked
- Nearly half of firms don't fear hackers
- What Is Next on Hackers' Hit Lists
- Custom Code for Targeted Attacks
- And The Hits Keep Coming
- Unplug Everything!
- The Big Attacks are Back…Not That They Ever Stopped
- Technology Can Only Do So Much

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

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