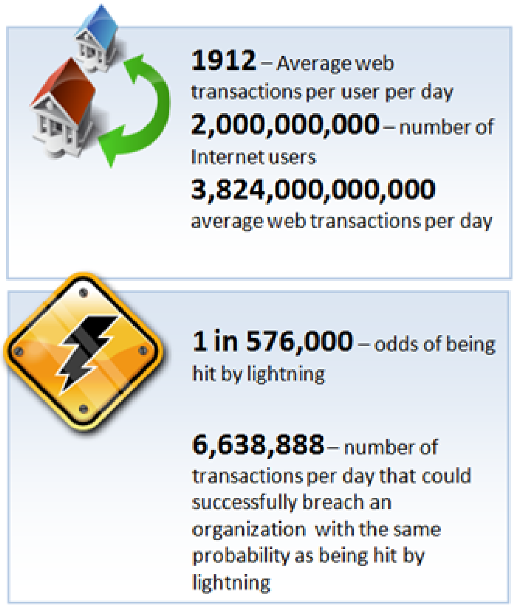
F5 Friday: If Only the Odds of a Security Breach were the Same as Being Hit by Lightning

Lori MacVittie, 2011-19-08

#v11 *AJAX, JSON and an ever increasing web application spread increase the odds of succumbing to a breach. BIG-IP ASM v11 reduces those odds, making it more likely you'll win at the security table*

When we use analogy often enough it becomes pervasive, to the point of becoming an idiom. One such idiom is the expression of unlikelihood of an event by comparing it to being hit by lightning. The irony is that the odds of being hit by lightning are actually fairly significant – about 1:576,000. Too many organizations view their risk of a breach as bring akin to being hit by lightning because they're small, or don't have a global presence or what have you. The emergence years ago of "mass" web attacks rendered – or should have rendered - such arguments ineffective. Given the increasing number of web transactions on the Internet and the success of web-based attacks to enact a breach, even comparing the risk to the odds of being hit by lightning does little but prove that eventually, you're going to get hit.



1912 – Average web transactions per user per day

2,000,000,000 – number of Internet users

3,824,000,000,000 average web transactions per day

1 in 576,000 – odds of being hit by lightning

6,638,888 – number of transactions per day that could successfully breach an organization with the same probability as being hit by lightning

Research by ZScaler earlier this year indicated an average (median) number of web transactions per day, per user at 1912. Analysts put the number of Internet users at about two billion. That translates into more than three trillion web transactions *per day*. Every day, three trillion transactions are flying around the web. Based on the odds of being hit by lightning, that means over 6 million of those transactions would breach an organization.

The odds suddenly aren't looking as good as they might seem, are they? If you think that's bad, you ain't read the most recent Ponemon results, which recently concluded that the odds of being breached in the next year were a "statistical certainty."

No, it's not paranoia if they really are out to get you and guess what? Apparently they are out to get you.

Truth be told, I'm not entirely convinced of the certainty of a breach because it assumes precautionary measures and behavior is not modified in the face of such a dire prediction. If organizations were to say, change their strategy as a means to get better odds, then the only statistical certainty would likely be that a breach would be attempted – but not necessarily be successful.

The bad news is that even if you have protections in place, the bad guys methods are evolving. If your primary means of protection are internal to your applications, the possibility remains that a new attack will require a rewrite – and redeployment. And even if you are taking advantage of external protection such as a web application firewall like BIG-IP ASM (Application Security Manager) it's possible that it hasn't provided complete coverage or accounted for what are misconfiguration errors: typographical case-sensitivity errors that can effectively erode protections.

The good news is that even as the bad guys are evolving, so too are those external protective mechanisms like BIG-IP ASM. BIG-IP ASM v11 introduced significant enhancements that provide better protection for emerging development format standards as well as address those operational oops that can leave an application vulnerable to being breached.

BIG-IP v11 Enhancements

- **AJAX and JSON Support**
  AJAX growth over the past few years have established it as the status quo for building interactive web applications. Increasingly these interaction exchanges via AJAX use JSON as their preferred data format of choice. Previous versions of BIG-IP ASM were unable to properly parse and therefore secure

JSON payloads.

A secondary issue with AJAX is related to the blocking pages generally returned by web application firewalls. For example, a BIG-IP ASM blocking page is HTML-based. When an AJAX embedded control triggers a policy violation, this means it can't present the blocking page because it doesn't expect to receive back HTML – it expects JSON. This leaves operators in the dark as it makes troubleshooting AJAX issues very difficult.

To address both these issues, BIG-IP ASM v11 can now parse JSON payloads and enforce proper security policies. This is advantageous not only for protecting AJAX-exchanged payloads, but for managing integration via JSON-based APIs from external sources. Being able to secure what is essentially third-party content is paramount to ensuring a positive security posture regardless of external providers' level of security. BIG-IP ASM v11 can also now also display a blocking page by injecting JavaScript into the response that will popup a window with a support ID, traceable by operators for easier troubleshooting. The ability to display a blocking page and ID is unique to BIG-IP ASM v11.

- **Case Insensitivity**
  Case sensitivity in general is derived from the underlying web server OS. While having a case sensitivity policy is an advantage on Unix/Linux platforms it can be painful to manage on other platforms. This is due to the fact that many times developers will write code without considering sensitivity. For example, a web server configured to serve a single file type, "html", may also need to configure Html, hTml, HTml, etc… because a developer may have fat-fingered links in the code with these typographical errors. On Windows platforms, this is not a problem for the application, but it becomes an issue for the web application firewall because it is sensitive to case necessarily. BIG-IP ASM v11 now includes a simple checkbox-style flag that indicates it should ignore case, making it more adaptable to Windows-based platforms in which case may be variable. This is important in reducing false positives – situations where the security device thinks a request is malicious but in reality it is not. As web application firewalls generally contain very granular, URI-level policies to better protect against injection-style attacks, they often flag case differences as being "errors" or "possible attacks." If configured to block such requests, the web application firewall would incorrectly reject requests for pages or URIs with case differences caused by typographical errors. This enhancement allows operators to ignore case and focus on securing the payload.
- **BIG-IP ASM VE**

  BIG-IP ASM is now available in a virtual form-factor, ASM VE. A virtual form-factor makes it easier to evaluate and test in lab environments, as well as enabling developers to assist in troubleshooting when vulnerabilities or issues arise that involve the application directly. Virtual patching, as well, is better enabled by a virtual form factor, as is the ability to deploy remotely in cloud computing environments.

There is no solution short of a scissors that can reduce your risk of breach to 0. But there are solutions that can reduce that risk to a more acceptable level, and one of those solutions is BIG-IP ASM. Getting hit by lightning on the Internet is a whole lot more likely than the idiom makes it sound, and anything that can reduce the odds is worth investigating sooner rather than later.

More BIG-IP ASM v11 Resources:

- Application Security in the Cloud with BIG-IP ASM
- Securing JSON and AJAX Messages with F5 BIG-IP ASM
- BIG-IP Application Security Manager Page
- Audio White Paper - Application Security in the Cloud with BIG-IP ASM

- F5 Friday: You Will Appsolutely Love v11
- SQL injection – past, present and future
- Introducing v11: The Next Generation of Infrastructure

- BIG-IP v11 Information Page
- F5 Monday? The Evolution To IT as a Service Continues … in the Network
- F5 Friday: The Gap That become a Chasm
- All F5 Friday Posts on DevCentral
- ABLE Infrastructure: The Next Generation – Introducing v11