Using F5's iRules to Prevent Your Web Site From Being Phished

Overview

Phishing scams have become a sad fact of life – but developers can stop them, with a little help. If you own F5's BIG-IP Local Traffic Manager running version 9 or later, you already have the ability to make use of F5's custom, in-line scripting language, iRules. And now there's a new iRule available that has been designed to help stop phishing in its tracks.

Challenge

We've all seen one: an email falsified to appear as if it's from a reputable bank or financial institution. Maybe it wasn't a bank, maybe it claimed to be from the IRS or your online stock trader of choice. Regardless, the intent is the same: They want access to your account, and all they need you to do is provide some small piece of information. Sometimes it's your Social Security number, other times it's your account number or perhaps your username and password. The email asks for this by saying there's been some major change, or that you need to update your account information. Whatever information they're phishing for; wouldn't your customers be a lot happier if you could help prevent this from happening?

With iRules and BIG-IP Local Traffic Manager v9, you can.

Solution

iRules are customizable commands that leverage the power of the BIG-IP product's TMOS architecture. iRule functionality is delivered in conjunction with the BIG-IP system and allows developers and network professionals to create and customize policies that provide direct, granular control over how the BIG-IP system directs application traffic at any moment within the application transaction or flow. Based on a proven programming language (Tool Command Language or TCL), iRules can be applied to any IP application or protocol, enabling new degrees of application optimization and security. Furthermore, iRules can be invoked and manipulated via F5's unique iControl web services API, allowing the network to do things that previously required changes in applications.

How It Works

To perform phishing attacks, malicious code is used to replicate the site of the company whose customers the attacker wants to scam, and then sends unsuspecting customers to this site in order to gather sensitive personal information. Using a BIG-IP system and iRules, you can help to prevent this type of attack from occurring.

The following example demonstrates not only how to check for suspicious requests that originate from a referrer that hasn't been authorized to use your site's content, but how to either stop them outright, or inject code into the HTTP response to help negate their ability to duplicate your site. This is done in three separate steps.

Note: *The following examples contain example code which shows how you can leverage your BIG-IP v9 and iRules to offer a vast array of ways to secure and optimize your applications and data. This is just a single example of the types of solutions iRules can provide. The true power lies in the flexibility of the language which allows you to custom craft solutions to meet your exact needs.*

1. Define a list of valid referrers in the form of a class. This is a list of those sites that you expect to be linking to content on your site. For example:

```
class valid_referers {
  http://mydomain.com
  http://mydomain1.com
  http://url1
  http://url2
  http://url3
}
```

2. Define a list (in the form of a class) of file types that should not be linked to, except by the referrers listed in item #1. For example:

```
class file_types {
  ".gif"
  ".jpg"
  ".png"
  ".bmp"
  ".js"
  ".css"
  ".xsl"
}
```

3. Check to see if an invalid referrer (not someone in class #1) is trying to serve data from your site and what kind of content they're trying to serve. If it matches the file types in Class #2, block it. If not, insert some custom code to help prevent phishing attempts. The following example is an iRule that performs this functionality:

```
rule no_phishing {
  when HTTP_REQUEST {
    # Don't allow data to be chunked.
    if {[HTTP::version] == "1.1"} {
      if {[HTTP::header is_keepalive]} {
        # Adjust the Connection header.
        HTTP::header replace "Connection" "Keep-Alive"
      }
      HTTP::version "1.0"
    }

    if { [matchclass [HTTP::header "Referer"] starts_with
$::valid_referers] < 1 } {
      if { ([string tolower [HTTP::method] ] eq "get") &&
([matchclass [HTTP::uri] contains $::file_types] > 0 )} {
        discard
      } elseif { ([HTTP::header exists "Content-Type"]) &&
([HTTP::header "Content-Type"] starts_with "text" ) } {
        set respond 1
      }
    }
  }

  when HTTP_RESPONSE {
    if { $respond == 1 } {
      if { [HTTP::header exists "Content-Length"] } {
        set content_len [HTTP::header "Content-Length"]
      } else {
        set content_len 4294967295
      }

      if { $content_len > 0 } {
        HTTP::collect $content_len
      }
    }
  }

  when HTTP_RESPONSE_DATA {
    set bypass [string first -nocase "<html>" [HTTP::payload] ]
    if { $bypass != -1 } {
      HTTP::payload replace $bypass 0 "<script
type=\"text/javascript\">\n if (top.frames.length!=0) {\n if
(window.location.href.replace)\n
top.location.replace(self.location.href);\n
else\n top.location.href=self.document.href;\n }\n </script>\n"
      } else {
      HTTP::respond 500
    }
  }
}
```

More information about this solution is available on F5’s DevCentral site, http://devcentral.f5.com/. DevCentral also contains a video where F5 engineers explain how to prevent your web site from being phished: http://devcentral.f5.com/weblogs/dctv/archive/2006/01/16/iRulesNoPhishing.aspx.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5’s extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.