

## Usando as iRules da F5 para impedir ataques phishing contra o seu website

**Visão Geral** Os golpes de phishing se tornaram um triste fato da vida - mas, com alguma ajuda, os desenvolvedores podem impedi-los. Se você possui o BIG-IP Local Traffic Manager da F5, executando a versão 9 ou mais recente, tem a capacidade de usar a linguagem personalizada de scripts da F5, chamada de iRules. Agora, há uma nova iRule disponível, criada especificamente para ajudar a deter os ataques de phishing.

**Desafio** Todos nós já vimos: um e-mail falso, que parece vir de um banco ou instituição financeira respeitável. Talvez não seja um banco. Ele pode alegar ser do imposto de renda, do seu corretor de ações on-line. Seja lá qual for, a intenção é a mesma: Eles querem acesso à sua conta, e tudo do que eles precisam é que você forneça umas poucas informações. Às vezes, é o seu número do seguro social; outras, pode ser o número da sua conta, ou talvez seu nome de usuário e senha. O e-mail pede isso dizendo que houve uma mudança importante, ou que você precisa atualizar as informações da sua conta. Seja qual for a informação que eles estão procurando, será que os seus clientes não ficariam muito mais satisfeitos se você pudesse ajudá-los a impedir esse tipo de coisa?

Com as iRules e o BIG-IP Local Traffic Manager v9, você pode.

**Solução** As iRules são comandos personalizáveis que empregam todo o poder da arquitetura TMOS, dos produtos BIG-IP. A funcionalidade das iRules é fornecida em conjunto com o sistema BIG-IP e permite aos desenvolvedores e profissionais de rede criar e personalizar políticas que oferecem um controle direto e granular sobre como o sistema BIG-IP direciona o tráfego de aplicativos, a qualquer momento, durante o fluxo ou transação do aplicativo. Baseado em uma linguagem consagrada de programação (Tool Command Language, TCL), as iRules podem ser aplicadas a qualquer aplicativo ou protocolo IP, habilitando novos níveis de otimização e segurança de aplicativos. Além disso, as iRules podem ser invocadas e manipuladas pela API de serviços web iControl, exclusiva da F5, permitindo que a rede possa fazer coisas que, de outra forma, exigiriam mudanças nos aplicativos.

### **Como funciona**

Para executar os ataques phishing, o código malicioso é usado para replicar o site da companhia cujos clientes o atacante deseja fraudar e, então, direciona usuários insuspeitos para esse site, para coletar informações pessoais sigilosas. Usando um sistema BIG-IP e as iRules, você pode ajudar a impedir que esse tipo de ataque aconteça.

O exemplo a seguir demonstra não somente como checar por solicitações suspeitas, originadas por um referer que não tem autorização para usar o conteúdo do seu site, mas também como impedi-los imediatamente ou como injetar um código na resposta HTTP para ajudar a negar a capacidade de duplicação do seu site. Isso é feito em três passos diferentes.

**Nota:** *Os exemplos a seguir mostram os códigos que ajudam você a empregar o BIG-IP v9 e as iRules para oferecer uma vasta gama de opções de segurança, além de otimizar seus aplicativos e dados. Esse é apenas um exemplo dos tipos de soluções que as iRules podem fornecer. A verdadeira força reside na flexibilidade da linguagem, que lhe permite criar soluções personalizadas para atender às suas necessidades específicas.*

1. Defina uma lista de referrers válidos, na forma de uma classe. Essa é uma lista dos sites que podem ter links para o conteúdo do seu site. Por exemplo:

```
class valid_referers {
  http://meudominio.com
  http://meudominio1.com
  http://url1
  http://url2
  http://url3
}
```

2. Defina uma lista (também em forma de classe) de tipos de arquivos que não podem ser vinculados, exceto pelos referrers listados no item 1. Por exemplo:

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

3. Verifica se um referrer inválido (que não consta na classe nº 1) está tentando servir dados do seu site, e qual tipo de conteúdo ele está tentando distribuir. Se for algum dos tipos de arquivo definidos na classe nº 2, bloqueia a solicitação. Se não, insere código personalizado para ajudar a impedir as tentativas de phishing. O exemplo a seguir é uma iRule que executa essa funcionalidade:

```
#Ajustar o cabeçalho de conexão.
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
}
}
}
```

Mais informações sobre essa solução podem ser encontradas no site DevCentral da F5, no endereço <http://www.devcentral.f5.com> (em inglês). O DevCentral também contém um vídeo em que os engenheiros da F5 explicam como impedir que o seu website sofra ataques phishing.

<http://devcentral.f5.com/weblogs/dctv/archive/2006/01/16/iRulesNoPhishing.aspx>.

### **Sobre a F5**

A F5 Networks é a líder global em Application Delivery Networks. A F5 fornece soluções que tornam os aplicativos seguros, rápidos e disponíveis para todos, ajudando as companhias a obter o maior retorno pelo seu investimento. Ao implementar inteligência e gerenciabilidade na rede para transferir a carga de aplicativos, a F5 os otimiza, permitindo que eles trabalhem mais rápido e consumam menos recursos. A arquitetura expansível da F5 integra de forma inteligente a otimização de aplicativos, protege os aplicativos e a rede e oferece confiabilidade aos aplicativos - tudo em uma plataforma universal. Mais de 10.000 companhias e provedores de serviços em todo o mundo confiam na F5 para manter seus aplicativos funcionando. A companhia tem sede em Seattle, Washington, com escritórios no mundo todo. Para mais informações, visite [www.f5.com](http://www.f5.com) (em inglês).