GUIA BÁSICO PARA CAMPANHAS PHISHING

1. CRIANDO MENSAGENS EFETIVAS

Este guia mostra técnicas para a criação de mensagens para testes phishing via e-mail. Da identificação de um domínio vulnerável – ou criação de um falso – até a construção a construção da mensagem utilizando os mesmos padrões de um e-mail verdadeiro. Em um próximo artigo, veremos técnicas e o funcionamento de testes de spear-phishing.

Buscando Domínios Vulneráveis

A melhor forma de entregar mensagens falsas se dá mediante a exploração de vulnerabilidades em servidores smtp. Destre elas, existem dois tipos interessantes para nosso propósito:

- 1) Erros de *parsing* ocorrem por falhas no tratamento das mensagens. Podem ocorrer diretamente nos filtros da implementação do protocolo ou na interface de usuários legítimos.
- 2) Falhas de *mail spoofing* devido à má configuração. Focaremos nesta falha por ser facilmente explorada e não requerer um ambiente de testes complexo.

Não faz parte do escopo deste artigo discorrer sobre os detalhes técnicos de uma falha de *mail spoofing*. No momento, basta saber que configurações inseguras de *SPF*, *DMARC* e/ou *DKIM* podem fazer com que um servidor de e-mails não verifique a autenticidade das mensagens a serem enviadas. Desta forma, qualquer pessoa pode enviar mensagens em nome do domínio afetado.

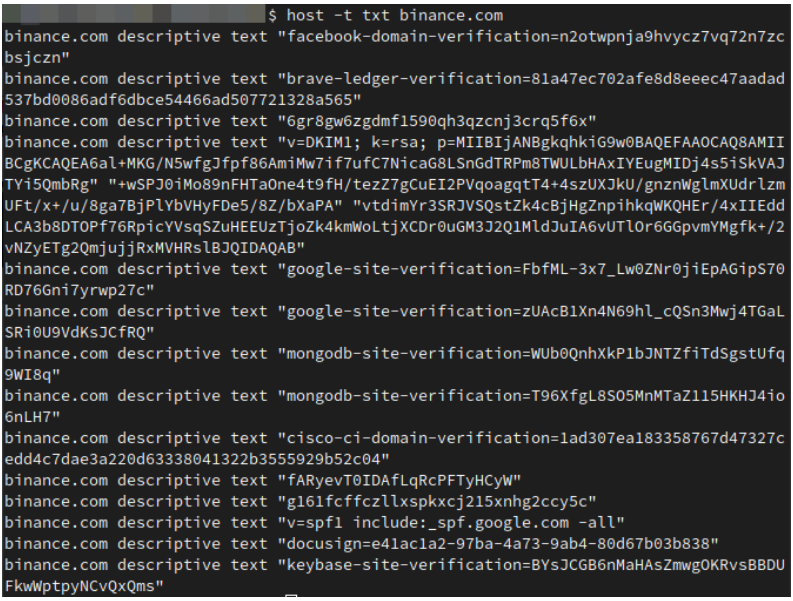
Existem várias formas de detectar se um domínio está vulnerável à mail spoofing. Uma delas é checar os registros de texto do domínio. Você pode fazer isto utilizando o utilitário **host** em ambientes Linux:

```
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] [-p port] hostname [server]
       -a is equivalent to -v -t ANY
       -A is like -a but omits RRSIG, NSEC, NSEC3
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -p specifies the port on the server to query
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -U enables UDP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
```

A opção **-t** nos permite realizar diversas consultas aos registros do domínio. Especificamente os argumentos **txt** e **mx**. ***Utilizaremos como exemplo o domínio binance.com. É preciso frisar que o domínio está seguro e que, ao final deste texto, não utilizaremos a mensagem criada.*** O comando **mx** nos retorna a localização dos servidores smtp de um domínio:

```
[redacted]$ host -t mx binance.com
binance.com mail is handled by 10 aspmx2.googlemail.com.
binance.com mail is handled by 5 alt1.aspmx.l.google.com.
binance.com mail is handled by 1 aspmx.l.google.com.
binance.com mail is handled by 5 alt2.aspmx.l.google.com.
binance.com mail is handled by 10 aspmx3.googlemail.com.
```

Já o comando **txt** retornará todos os registros das configurações deste domínio:



Note a tag de permissão *-all*. Ela indica que o domínio possui métodos de testar a autenticidade das mensagens em seu servidor smtp. Ao executar o comando txt em um domínio vulnerável, você poderá encontrar a resposta "*domain has no TXT record*" ou as tags de permissão *?all*, *~all*. Porém, a tag ~all por si não representa vulnerabilidade, é necessária investigação.

Criando seu Próprio Domínio

Suponhamos que você tenha visitado todos os domínios interessantes para o ataque, mas todos eles estão seguros. A solução é criar seu próprio domínio fantasma, que será usado somente para forjar um endereço de e-mail.

Embora os domínios desejados estejam seguros, eles não são imunes à personificação. Isto é, a criação de um domínio que se passe pelo original. Para dar mais credibilidade ao ataque, você precisa de um nome homóglifo, ou o mais próximo disto possível. Se o seu provedor de domínios não possuir um bom filtro de caracteres, você poderia, por exemplo, registrar em seu nome o domínio *binance.com*. Consegue identificar a diferença?

```
"binance.com" == "binance.com"
False
```

Neste exemplo, substituímos a letra c pelo charactere “c”. Ambos são homóglifos. Ou seja, possuem a mesma grafia, mas são tratados como caracteres diferentes. Você pode encontrar várias listas de homóglifos neste repositório. Ele também possui listas divididas para objetivos distintos: https://github.com/codebox/homoglyph

Uma forma de automatizar este processo é utilizando o utilitário **urlcrazy**. Além de gerar nomes alternativos para um domínio informado, ele fará uma validação automática para verificar se já existem domínios registrados em nome das variações criadas:

```
[redacted]$ ./urlcrazy binance.com
URLCrazy Domain Report
Domain    : binance.com
Keyboard  : qwerty
At        : 2022-07-27 11:02:33 -0300

# Please wait. 110 hostnames to process

Typo Type              Typo           DNS-A            CC-A                            DNS-MX                            Extn
---------------------------------------------------------------------------------------------------------------------------------
Character Omission     biance.com     82.156.163.191   NL,NETHERLANDS                                                    com
Character Omission     binace.com     47.52.200.94     CA,CANADA                                                         com
Character Omission     binanc.com     68.68.98.160     US,UNITED STATES                                                  com
Character Omission     binance.cm     185.206.180.117                                                                    cm
Character Omission     binane.com     166.88.19.180                                                                      com
Character Omission     binnce.com                      ?                                                                 com
Character Omission     bnance.com     23.227.38.32                                                                       com
Character Repeat       bbinance.com   47.52.200.94     CA,CANADA                                                         com
Character Repeat       biinance.com   166.88.19.181                                                                      com
Character Repeat       binaance.com   166.88.19.180                                                                      com
Character Repeat       binancce.com   166.88.19.180    IR,IRAN (ISLAMIC REPUBLIC OF)                                     com
Character Repeat       binancee.com   199.59.243.220   ES,SPAIN                                                          com
Character Repeat       binannce.com   166.88.19.181                                                                      com
Character Repeat       binnance.com   68.68.98.160     US,UNITED STATES                                                  com
Character Swap         biannce.com    166.88.19.181                                                                      com
Character Swap         binacne.com    68.68.98.160     US,UNITED STATES                                                  com
```

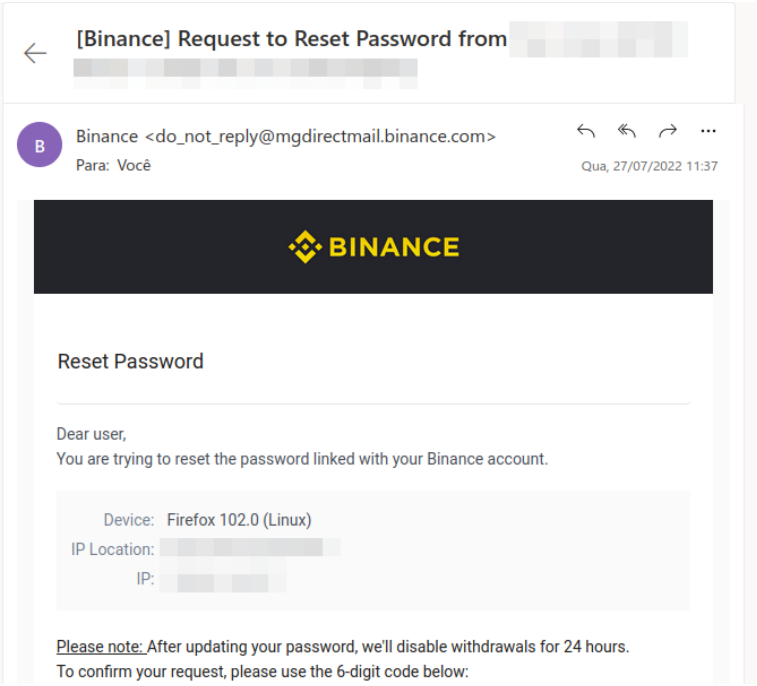
Durante o processo, o urlcrazy poderá encontrar também os servidores de e-mail verdadeiros. Não é incomum que empresas registrem domínios com variações do próprio nome, para evitar este tipo de ataque. Por exemplo, o domínio gooogle.com também pertence à Google e redireciona o usuário para o site principal.

O urlcrazy pode ser baixado pelo repositório: https://github.com/urbanadventurer/urlcrazy

Coletando o Modelo de Mensagem

Você já possui um domínio pronto para uso. Seja ele o original, com falhas de segurança, ou clonado. No entanto, antes de enviar sua mensagem você precisa identificar o padrão de texto usado pela compania. O objetivo é criar a mensagem mais realista possível, portanto, quanto mais amostras das mensagens originais você obtiver, melhor.

Uma das formas de coletar amostras é utilizando as mensagens fornecidas pelo domínio de modo autônomo. *Newslleters*, campanhas de marketing e interfaces de interação automatizada são alvos perfeitos. Em nosso caso, requisitaremos um e-mail de alteração de senha em https://accounts.binance.com/en/user/reset-password . Alguns minutos depois, recebemos a seguinte mensagem:


[Binance] Request to Reset Password from

B

Binance <do_not_reply@mgdirectmail.binance.com>

Para: Você

Qua, 27/07/2022 11:37

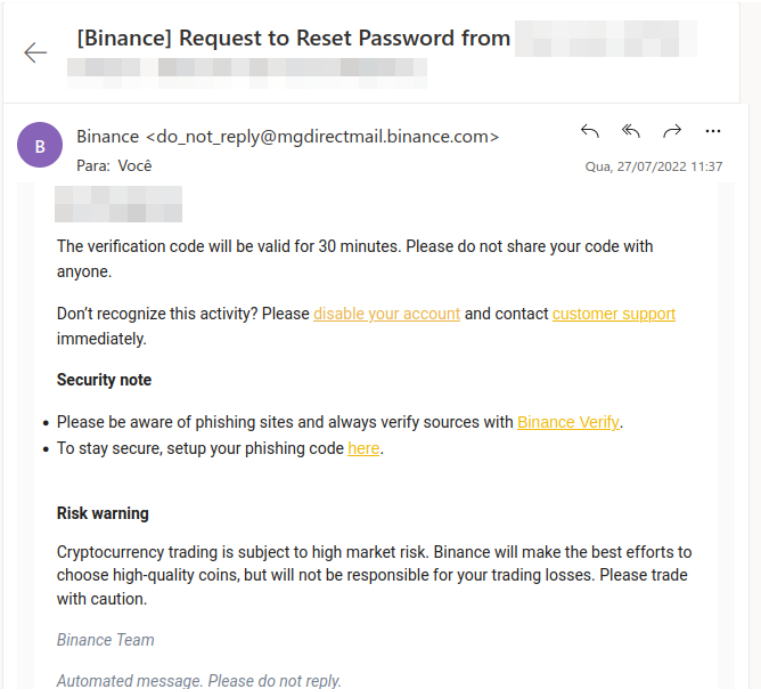
BINANCE

Reset Password

Dear user,
You are trying to reset the password linked with your Binance account.

Device: Firefox 102.0 (Linux)
IP Location:
IP:

Please note: After updating your password, we'll disable withdrawals for 24 hours.
To confirm your request, please use the 6-digit code below:



[Binance] Request to Reset Password from [redacted]

B Binance <do_not_reply@mgdirectmail.binance.com>

Para: Você

Qua, 27/07/2022 11:37

[redacted]

The verification code will be valid for 30 minutes. Please do not share your code with anyone.

Don't recognize this activity? Please disable your account and contact customer support immediately.

Security note

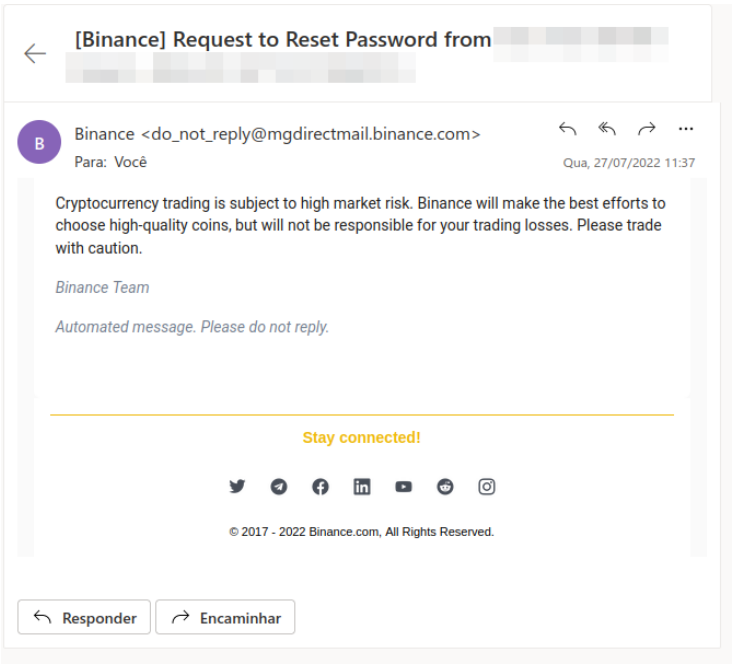
- Please be aware of phishing sites and always verify sources with Binance Verify.
- To stay secure, setup your phishing code here.

Risk warning

Cryptocurrency trading is subject to high market risk. Binance will make the best efforts to choose high-quality coins, but will not be responsible for your trading losses. Please trade with caution.

Binance Team

Automated message. Please do not reply.



[Binance] Request to Reset Password from [redacted]

B Binance <do_not_reply@mgdirectmail.binance.com>

Para: Você

Qua, 27/07/2022 11:37

Cryptocurrency trading is subject to high market risk. Binance will make the best efforts to choose high-quality coins, but will not be responsible for your trading losses. Please trade with caution.

Binance Team

Automated message. Please do not reply.

Stay connected!

Responder Encaminhar

Além do corpo da mensagem, outros pontos importantes são o endereço de envio - você precisará dele para explorar o *spoofing* ou terá de criar um similar, no seu domínio falso -, e o assunto da mensagem. Será necessário que o seu e-mail siga o mesmo padrão.

Utilize as ferramentas de inspeção do seu navegador para extrair o código HTML do e-mail, e pronto! Você possui uma mensagem idêntica às mensagens verdadeiras.

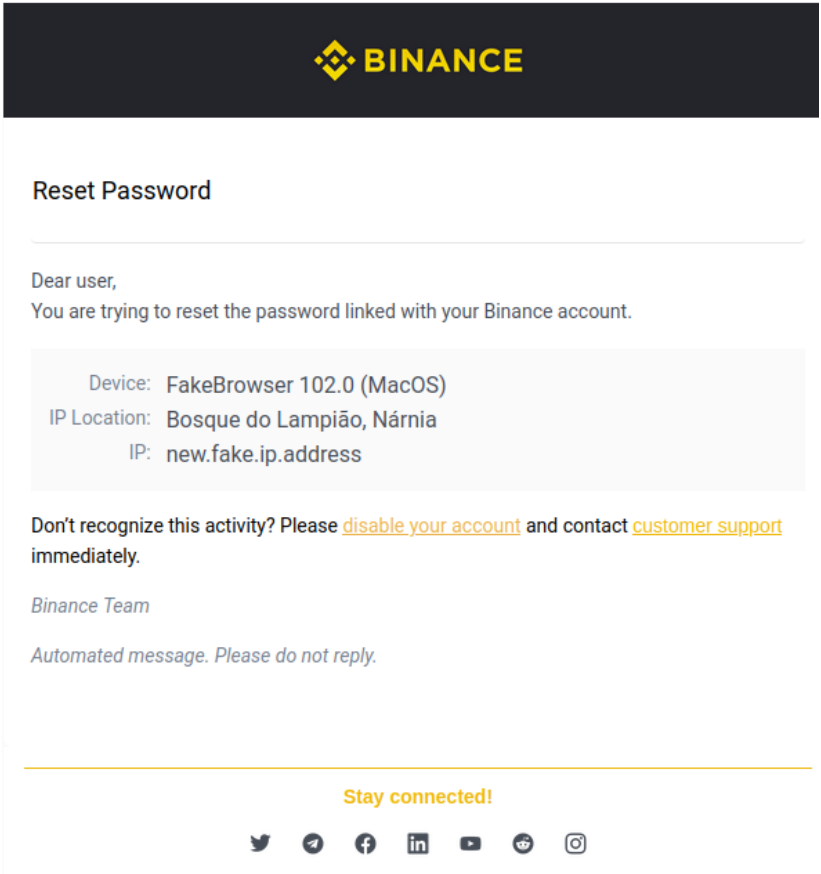
Modificando a Mensagem

Existem duas abordagem nesta etapa. Você pode:

- Utilizar a mensagem tal como ela é, alterando somente os parâmetros individuais de cada destinatário, quando houver. São eles nome, endereço de e-mail e qualquer outra informação referente à conta individual do cliente. Altere também todos os links da mensagem para links maliciosos cujas conexões você tenha controle. Uma dica é não utilizar o mesmo link em todas as tags, pois mecanismos de segurança podem identificar este comportamento como malicioso.

- A segunda abordagem é utilizar o padrão da mensagem para criar um texto novo, adaptado ao seu cenário e propósito. Tendo extraído o código HTML da mensagem, esta tarefa é fácil e não deve tomar mais de alguns minutos.

Optando pela segunda rota, aqui vai um exemplo de mensagem alterada seguindo os padrões da original:



Note que modificamos ligeiramente alguns textos e removemos bastante conteúdo. Uma edição básica apenas para demonstrar que, tendo posse da mensagem, você pode transformá-la da forma que preferir.

Enviando a Mensagem

Por questões legais, não cobriremos aqui o envio da mensagem. Para isto, teríamos de identificar uma compania vulnerável à spoofing e explorar a vulnerabilidade. Como não é o caso do nosso exemplo, nem registramos um domínio falso para nos passarmos por ele, nossa parte prática termina aqui.

Dicas Extras

- Mesmo quando não se tratar de *spear-phishing*, procure selecionar domínios que tenham alguma relação com os alvos. Ponto extra se for de um serviço que eles utilizem. Se apropriado, crie uma mensagem falsa se passando pela própria empresa onde os alvos trabalham.

- Por falar em serviço, dê preferência à serviços e plataformas que enviem notificações primariamente via e-mail. Redes sociais em geral tendem à notificar os usuários por alertas em dispositivos móveis, logo não são um bom vetor de ataque. Excetuadas as mensagens de alterações na conta.

- Ao inserir links maliciosos nas mensagens, esconda-os com encurtadores para que não seja possível identificar o destino apenas analisando o código do e-mail.

- Uma excelente ferramenta para o envio de mensagens em massa é o GoPhish. Embora eu recomende, no caso de mail spoofing, que você crie seu próprio código, o GoPhish é uma das melhores soluções quando se fala do envio (com monitoramento) de mensagens em massa. Saiba mais sobre ele em https://getgophish.com/ . Existe uma versão

modificada com a alteração de alguns metadados. Ela pode ser útil quando os mecanismos de defesa dos alvos estão identificando suas mensagens como maliciosas: https://github.com/puzzlepeaches/sneaky_gophish .

Mais artigos, possivelmente, em https://www.linkedin.com/in/rf-peixoto/ . Se este artigo foi útil, considere doar um café para a chave Pix abaixo. :)

05a40344-532b-484f-bab3-1da4f27e75b6