Fraude personificando a marca Continente espalha-se através do WhatsApp: Não se deixe enganar!

seguranca-informatica.pt/fraude-personificando-a-marca-continente-espalha-se-atraves-do-whatsapp-nao-se-deixe-enganar/

August 27, 2021

Nos últimos dias, uma nova campanha fraudulenta personificando a marca Continente tem atingido os utilizadores portugueses. A campanha tem a capacidade de se auto-propagar via WhatsApp.

Uma nova campanha fraudulenta personificando a marca Continente está a ser disseminada em Portugal poucos dias antes do final do mês de agosto de 2021. Os malfeitores utilizam uma *landing page* totalmente responsiva a dispositivos móveis com uma mensagem referente à comemoração dos 40º aniversário da marca Continente.

A Figura 1 abaixo apresenta a *landing-page* da campanha capturada no dia 26 de agosto de 2021.

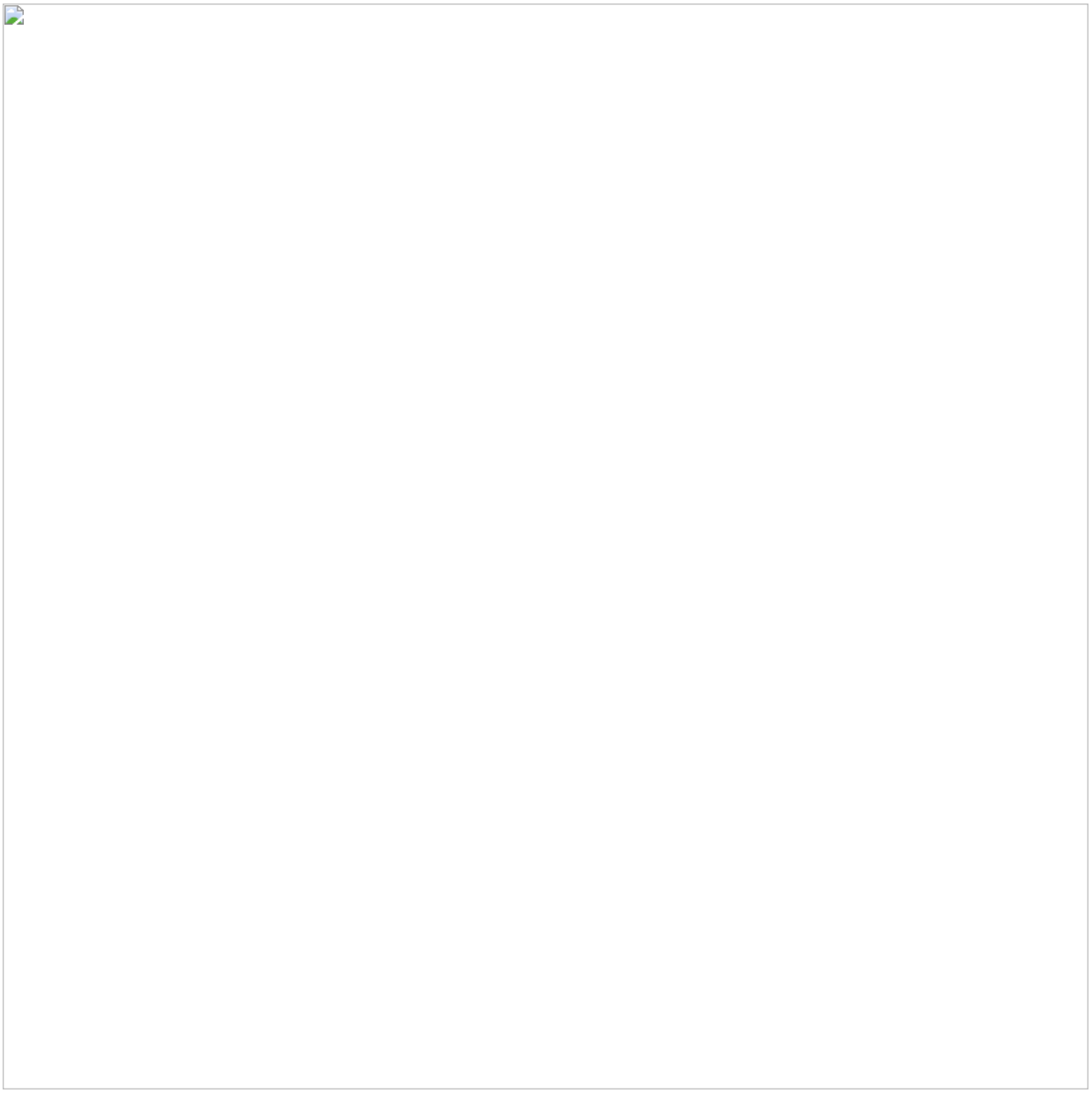


Figura 1: *Landing page da campanha maliciosa personificando a marca Continente (26-08-2021).*

Os malfeitores deixam uma mensagem principal como isco e escrita em bom português:

Comemoração do 40º aniversário! Através do questionário terá a oportunidade de ganhar um vale-presente Continente no valor de 800 euros. De forma a estabelecer um traço de legitimidade, são deixados também comentários falsos de maneira a motivar a vítima a prosseguir com o processo de recolha de dados.

Seguidamente, são apresentadas 4 questões à vítima, mas o seu conteúdo parece não ser capturada pela página; no fundo faz parte do chamariz do esquema.

Figura 2: *Questões entregues à vítima pelos malfeitores de forma a tornar o esquema o mais real possível.*

Pode observar-se que nesta fase já são identificáveis traços de uma gramática e escrita de origem brasileira. Após concluir esta etapa, é apresentado um ecrã indicando que a vítima ganhou um vale de compras em cartão no total de 800 euros.

No entanto, para prosseguir, a vítima terá que “compartilhar com 5 grupos / 20 amigos” a campanha maliciosa através da sua aplicação WhatsApp instalada no smartphone.

A cada clique no botão “**WhatsApp**“, é enviado um pedido através da aplicação WhatsApp com a URL da campanha como apresentado abaixo.

```
“whatsapp://send?text=https://URL”
```

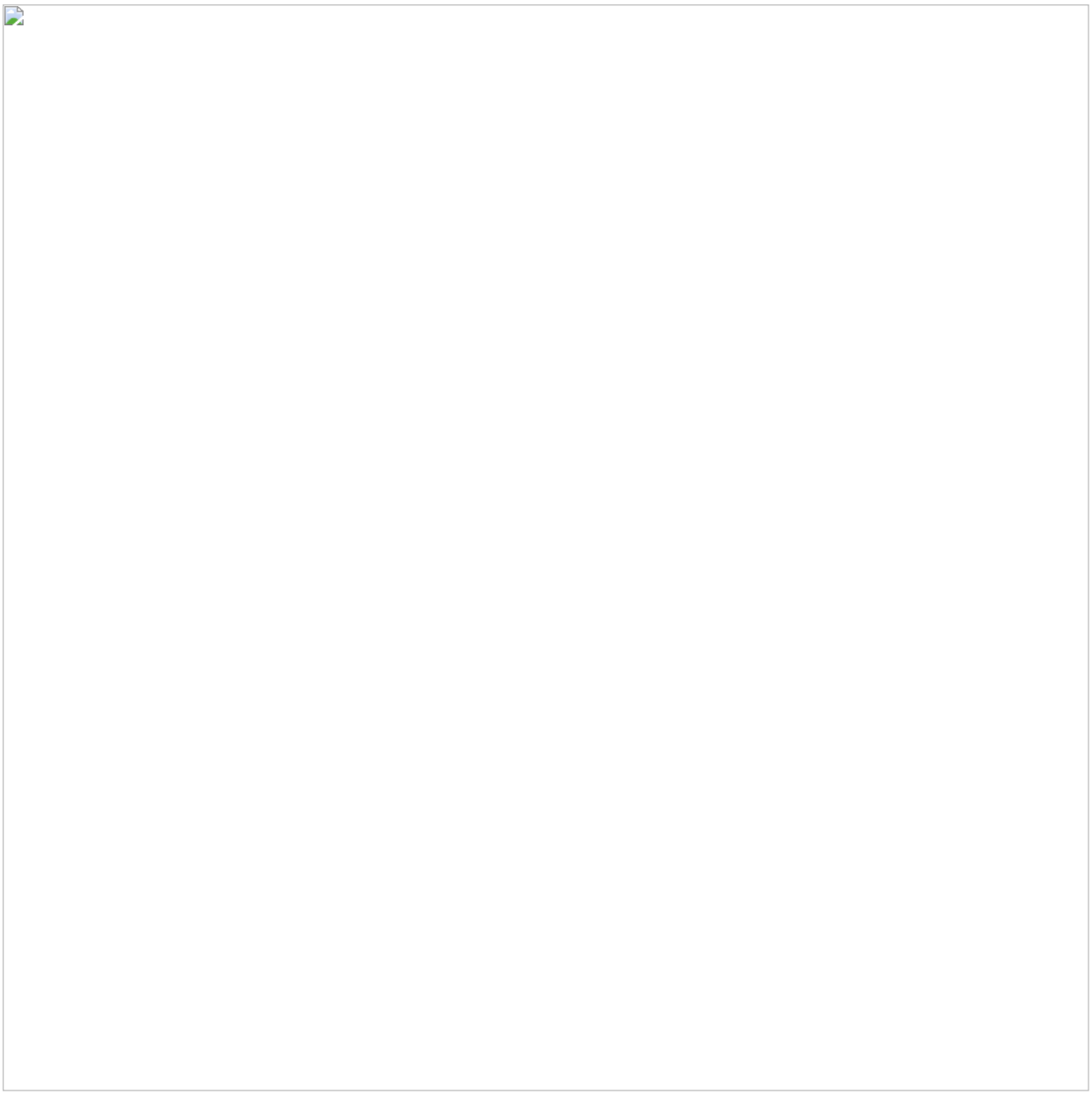
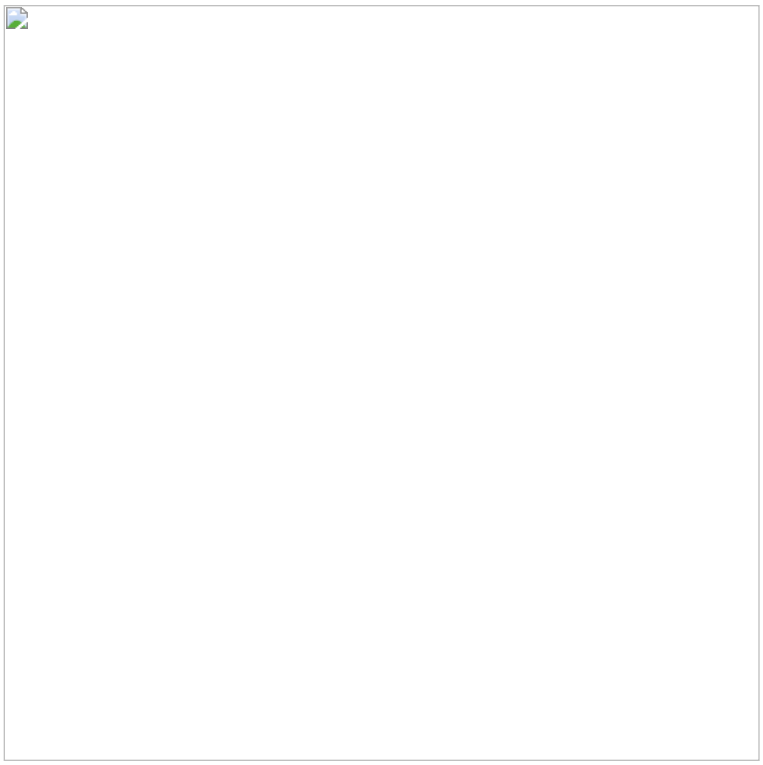


Figura 3: *Disseminação da campanha maliciosa através do WhatsApp.*

Após concluir a partilha um determinado número de vezes, o botão "**Prosseguir**" ficará ativo. Um trecho de código em JavaScript é responsável por incrementar o valor de uma variável denominada contador que compara o valor dessa variável com o limite de partilhas definido pelos malfeitores. Quando esse valor é atingido, o botão fica ativo no *layout* da aplicação.

Finalmente, a vítima é direcionada para a última página da campanha, a ponte com outras páginas maliciosas, onde é efetuada a recolha adicional de dados pessoais da vítima, cliques em anúncios, promoções, etc – uma forma de os malfeitores lucrarem efetivamente com esquemas desta natureza.



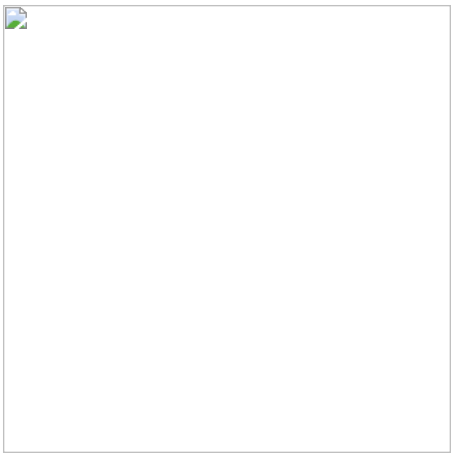


Figura 4: *Última página da campanha maliciosa, e onde a vítima é direcionada para outras páginas onde é realizada a recolha de dados pessoais, ads, etc.*

Curiosamente, esta não é uma campanha direcionada exclusivamente ao Continente e disseminada apenas em Portugal. Na Figura 5, podemos analisar que uma campanha com os mesmo traços está também em andamento, alojada no mesmo servidor, e utilizando o mesmo *modus operandi*.

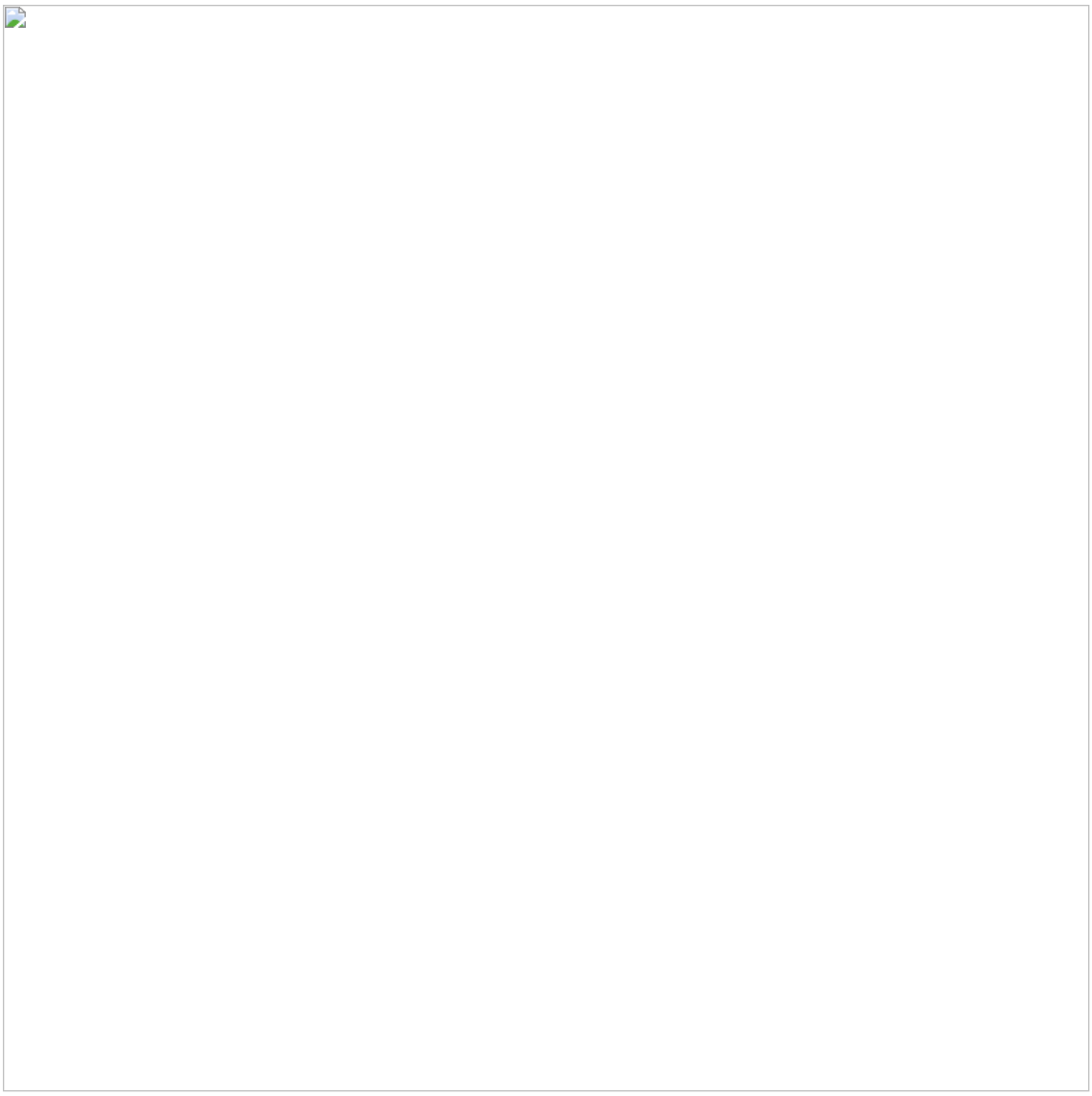


Figura 5: *Campanha maliciosa na língua inglesa disseminada pelos malfeitores.*

Todas as URLs e IoCs referentes a esta campanha foram submetidas no **0xSI_f33d**.

Aos utilizadores sugere-se uma vez mais, alguma sensibilidade e análise quando confrontados com situações desta natureza.

Todos os endereços foram adicionados ao ***0xSI_f33d*** para que as organizações possam proceder ao bloqueio dos endereços de IP/domínios de forma eficaz.

Em caso de suspeita de campanhas de phishing ou malware partilhe a situação com as autoridades ou através do **formulário disponível aqui**, ou submeta a URL maliciosa/suspeita para o **0xSI_f33d.**

Indicadores de Compromisso (IoCs)

```
hxxps://deviceviolin]top/continente/tb.php?_t=1629815531162981581497
hxxps://benignvan]xyz/Kpvn2uPU/continente/?_t=1630011784243#16300117
hxxps://weddingknock]top/continente/index.php
hxxps://developmandate]top/continente/tb.php?_t=16298810331629881191
hxxps://fascinatingquick]top/continente/tb.php?_t=162970844616297091
hxxps://chickenempty]top/continente/
hxxps://daringdevelop]top/continente/tb.php?_t=162997318216299734416
```

Submissões no 0xSI_f33d

https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2863
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2858
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2859
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2860
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2861
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2862
https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2863

Pedro Tavares
Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.