

Tracking Down the [A]pache Phishing Kit



CHECK POINT
RESEARCH

Cyberint
Protection Beyond the Perimeter

INTRODUCTION

In our latest research into the dark and dangerous world of phishing kits, Check Point Research and CyberInt have joined forces to show you how one of the most advanced phishing kits, the [A]pache Next Generation Advanced Phishing Kit, is currently being promoted and used on the Dark Net.

Allowing any aspiring cyber-criminal with very little knowledge to run a professional phishing campaign, our research outlines how the notorious [A]pache Phishing Kit is promoted online and instructs those looking to steal customers' credit card details by luring them to a fake shopping site.

A recent Check Point survey revealed that 65% of organizations have been prey to phishing attempts in a business context, with cyber-criminals often using the technique to gain access to an organization's network or sensitive information. As far as consumers are concerned, the target audience for [A]pache's efforts, it is their personal and financial credentials that are at stake.

Read the step by step guide below to see how [A]pache encourages and teaches his partners how to set up a sophisticated phishing scheme in minimal time, and the methods he uses to lure unsuspecting consumers into handing over their financial details.

Step 1: Access The Dark Web and Find [A]pache's Phishing Kit Advertisement

[A]pache makes it easy for those with very little technical ability to carry out their own cyber-attack. His cyber-criminal audience can simply download his multi-functioning phishing kit and following his installation instructions.

At \$100-\$300, the cost is higher than more standard phishing kits. Standard kits usually retail at \$20-\$50, with some even free, as they only provide login pages and prompts for personal and financial information. With [A]pache's next generation phishing kit however, threat actors are provided with a full suite of tools to carry out their attack. These include an entire back-office interface with which they can create convincing fake retail product pages and manage their campaign.

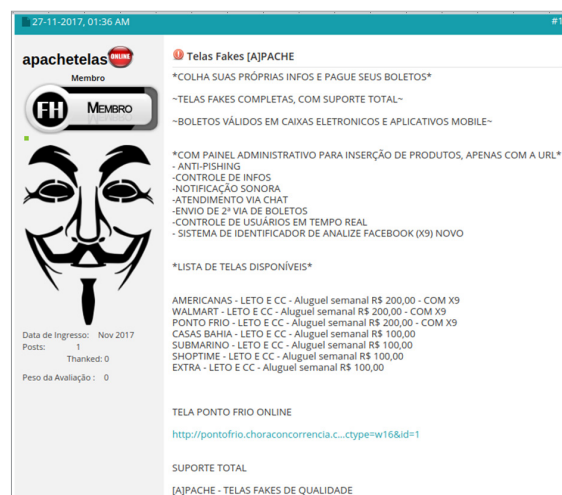


Figure 1: A posting on the Dark Net that advertises the [A]pache phishing kit.

Step 2: Choose a Retailer to Impersonate

[A]pache's phishing kit offers many well-known brands to choose from. Options include: Walmart, Americanas, Ponto Frio, Casas Bahia, Submarino, Shoptime and Extra. As most of these retailers are for a Brazilian audience, it seems this kit is aimed at those with a good knowledge of Portuguese, though we also found some kits that targeted US brands too.

Step 3: Register a Suitable Domain with Which to Lure Victims

In order to convincingly persuade their victims that they are shopping at the genuine site they think they are at, cyber-criminals also need a domain that is similar to the targeted brand, for example, www.walmart-shopping.com. Once registered, they are ready to deploy the kit to a PHP and MySQL supported web host, log in to the kit's admin panel and begin configuring their campaign.

Configuration options include:

- **Email:** Select the email address for notifications of new phished information to be sent to.
- **URL:** Select the URL upon which the phishing site sits.
- **Payments:** Choose to disable 'Boleto Bancário'¹ payments. This will force the potential victims to enter their credit card data, or display fake Boleto details.
- **Product Management:** Insert legitimate product URLs from the target retailer's website for automatic import and configure the display price to lure targets.
- **Victim Information Management:** Once the victims have been 'phished', their information can be displayed within the admin panel, both in full and as a list of credit card details.

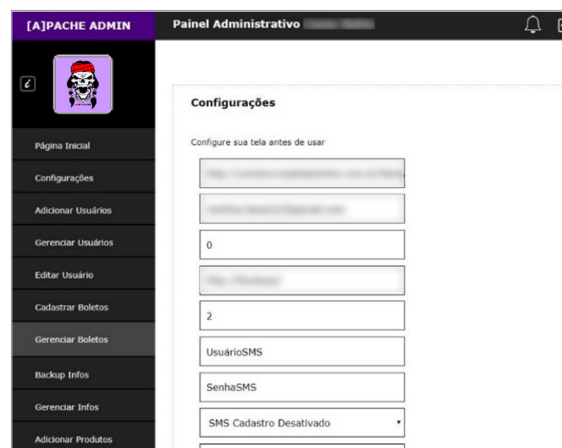


Figure 2: The phishing kit's admin panel.

¹ <https://en.wikipedia.org/wiki/Boleto>

Step 4: Add Products to the Fake Retail Site



Figure 3: Product price setting in the admin panel.

To simplify this process, [A]pache has made a simple user interface within the admin panel where the threat actor can paste the product URL of the legitimate retailer and the kit will automatically import the product information into the phishing page. They can then view their 'products' and change their original prices.

Step 5: Set Product Prices

Like any shop, the fake phishing site needs to also be competitive, so the product prices should aim to be attractive in order to motivate potential 'customers' to click on the items and proceed to checkout. Care needs to be taken here though as reducing prices too low though would raise suspicions with captivated 'customers'.

The cyber-criminal is now set to promote their site and lure in his victims.



Figure 4: The fake shopping website generated by the phishing kit.

Figure 5: Payment form as served by the phishing kit.

Step 6: Promoting the Site

Like any shop, the fake phishing site needs to also be competitive, so the product prices should aim to be attractive in order to motivate potential 'customers' to click on the items and proceed to checkout. Care needs to be taken here though as reducing prices too low though would raise suspicions with captivated 'customers'.

The cyber-criminal is now set to promote their site and lure in his victims.

[A]pache's next generation phishing kit also comes with an automated post-code look-up function to for added conviction.

Step 7: Check the Admin Panel

With payment details entered and sent straight to the threat actor's database, including the CVV number, they can then check the kit's back-office admin panel to see the victim's personal and financial information.

Meanwhile, after the victim has entered their payment details, they are presented with a notification that the payment process has failed. This helps convince them to not be concerned when the purchased fake product does not arrive.

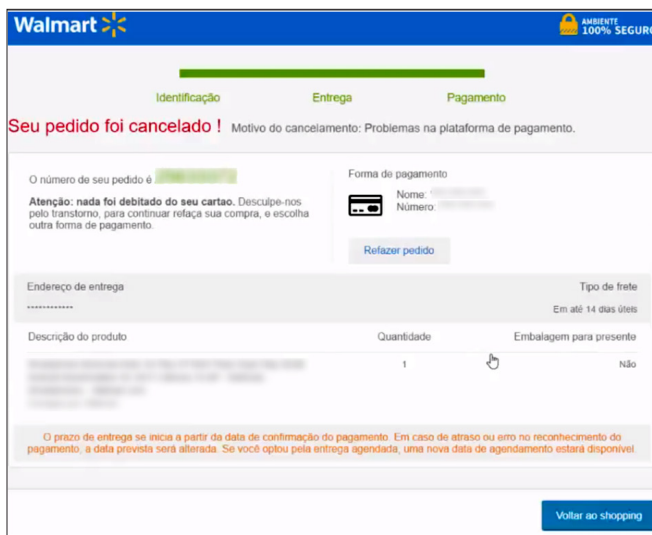


Figure 7: The payment error page shown to victim.

Dados da Vitima	
Nome Completo:	
Telefone: (55)	
CPF/CNPJ:	
E-mail:	
Senha:	
Testador Login:	
Endereço:	
Cidade / Estado:	
CEP:	

Dados do Cartão	
Titular Cartão:	
CPF Titular:	
Número Cartão:	
Número Cartão separado:	
Validade:	07/19
Código Segurança (cvv):	
Produto / Valor Smartphone	
Bin Checker:	Validação by: [A]PACHE

Figure 6: The admin panel collects victims' financial details.

Who Is [A]pache?

Our research team was able to find some hints and links to the possible entities behind this phishing kit.

For example, once an attack is over, cyber-criminals usually take down the fake retail site in order to lower the risks of being caught. In this case however, we found a custom built 'error 404' site in use.

This unique landing page was created by a web designer who is likely unaware that his work is being used for malicious purposes. While we did not notice any legitimate websites using this 404 page, and discovered that 'Blue World Electronics' does not actually exist, we did notice an English version of this page being used online. In fact, we found a few domains, serving PayPal phishing scams, using the English version of this page.

From this landing page we managed to find the actual phishing kit along with its admin panel. This led us to the next clue in discovering [A]pache's possible identity.



Figure 8: The error 404 page found in the phishing kit.

Looking into the kit's code, we discovered that [A]pache had included his handle, 'Douglas Zedn', in the control panel of the Walmart phishing site. This was either a mistake or he was looking for some kind of recognition for his work.

```
<html lang="pt-br">
<head>
<title>Painel Walmart 6.0|| Douglas Zedn</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
```

Figure 9: The The phishing kit's source code revealing [A]pache's handle.

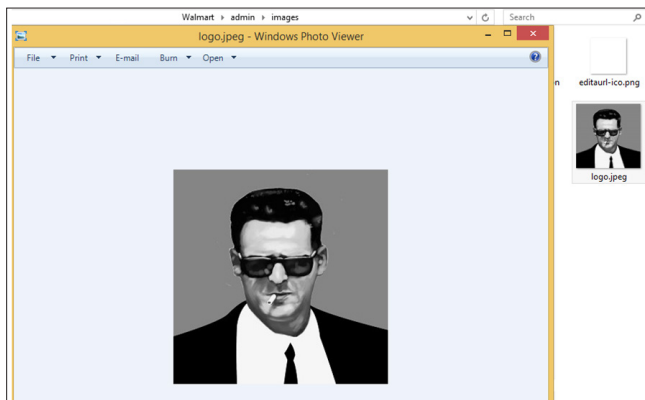


Figure 10: [A]pache's avatar as seen in his phishing kit's resources.

When carrying out a basic online search, as seen on his Steam social media profile page, we then discovered that 'Douglas' uses the same identity for his business life as he does for his personal life.



Figure 11: [A]pache's Steam social media profile.



Figure 12:
The real {A}pache...?

With one more step we were able to trace 'Douglas Zedn' back to his [Twitter handle](#). Could this be the real person behind the avatars?

Conclusion

Phishing attacks are one of the main methods used by threat actors to gain access to online retailers' data as well as a key way to directly target the customers who shop with them. The [A]pache phishing kit illustrates, however, the evolution that phishing kits are now undergoing in the fifth generation of the cyber threat landscape.

Protection against phishing is paramount for all organizations. To prevent malware coming into a network, organizations and consumers alike need 'Gen V' technologies to keep retail imposters at bay.

CyberInt Argos

[CyberInt's Argos](#)™ threat intelligence platform and Managed Detection and Response services allows their customers to combat and respond to advanced cyber threats that would normally go unnoticed by standard security controls, while protecting their brand, digital assets and customers. Learn more about [CyberInt Argos](#).

Check Point SandBlast Agent

[Check Point SandBlast Agent](#) provides purpose-built advanced Zero-Day Protection capabilities to web browsers and endpoints. Using Zero Phishing technology, SandBlast Agent proactively blocks access to new and unknown deceptive websites, as well as safeguards user credentials by preventing the use of corporate passwords on external websites. Learn more about [SandBlast Agent](#).

CHECK POINT
RESEARCH

CyberInt
Protection Beyond the Perimeter