MALWARE EVENT REPORT

Dolos-3PC

Series of innocuous advertisements that lead consumers to install backdoors and compromise devices for ongoing attacks

THE MEDIA TRUST
We know digital security.

Introduction

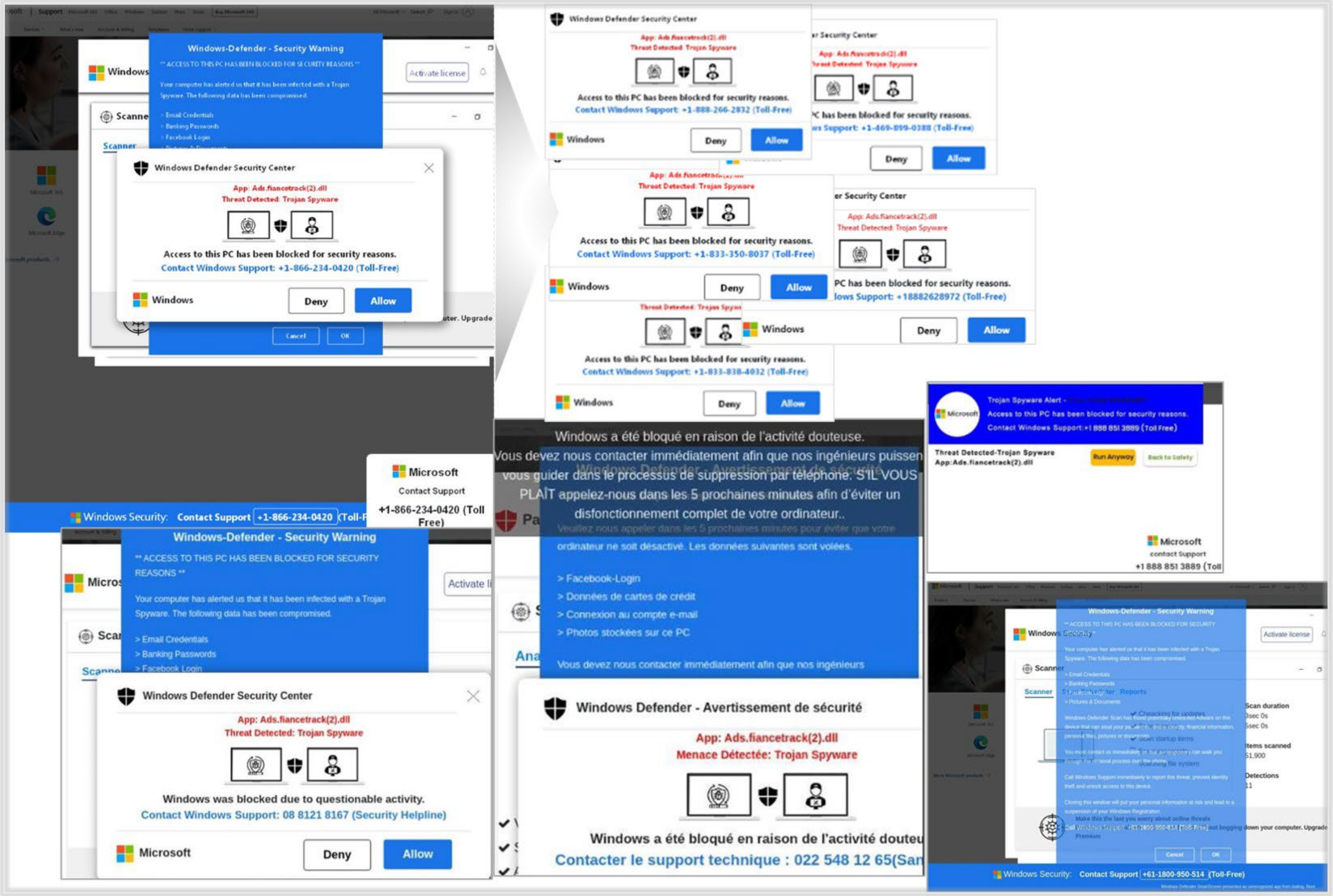
The Media Trust has been closely tracking an evolving malware campaign that uses a series of cloaked landing pages to serve fake virus pop ups. The delivery of this malware begins when a seemingly innocuous creative is served to the user. When clicked, the creative redirects the user to either a phony landing page or Windows-based virus alerts that presses the consumer to engage with a phony technical support operation. In the course of the engagement, consumers are presented with a fee to “clean” their device; however, it requires backdoor access to the device—which sets the stage for repeated attacks.

Dolos-3PC Attack Analysis

Dolos-3PC (Dolos) is an advertising-based malware campaign (aka “malvertising”) where the advertising ecosystem is the vector through which consumers are harmed. It is detected via client-side scanning of ad tags, websites, and creatives.

The recent spike began in May 2022, affecting at least four premium AdTech providers and more than 10 well-known media publishers. As of early July 2022, there are at least 30 distinct incidents attributed to different creative and landing page domain pairs, and the number continues to grow.

Key elements of this malicious campaign involve fake creatives (not associated with a known brand), a series of landing pages with varying degrees of legitimacy, device parameter checks, and cloaked redirects to popup virus alerts. If the correct conditions are met, the consumer is exposed to the malware in the form of fake virus alerts leveraging a well-known brand. [Figure 1]



Windows-Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

> Email Credentials
> Banking Passwords
> Facebook Login

Windows Defender Security Center

App: Ads.fiancetrack(2).dll
Threat Detected: Trojan Spyware

Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-866-234-0420 (Toll-Free)

Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-888-266-2832 (Toll-Free)

Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-469-899-0388 (Toll-Free)

Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-833-350-8037 (Toll-Free)

Access to this PC has been blocked for security reasons.
Contact Windows Support: +18882628972 (Toll-Free)

Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-833-838-4032 (Toll-Free)

Windows a été bloqué en raison de l'activité douteuse.
Vous devez nous contacter immédiatement afin que nos ingénieurs puissent vous guider dans le processus de suppression par téléphone. S'IL VOUS PLAÎT appelez-nous dans les 5 prochaines minutes afin d'éviter un disfonctionnement complet de votre ordinateur..

> Facebook-Login
> Données de cartes de crédit
> Connexion au compte e-mail
> Photos stockées sur ce PC

Vous devez nous contacter immédiatement afin que nos ingénieurs

Windows Defender - Avertissement de sécurité

App: Ads.fiancetrack(2).dll
Menace Détectée: Trojan Spyware

Windows a été bloqué en raison de l'activité douteu
Contacter le support technique : 022 548 12 65(San

Trojan Spyware Alert -
Access to this PC has been blocked for security reasons.
Contact Windows Support:+1 888 851 3889 (Toll Free)

Threat Detected-Trojan Spyware
App:Ads.fiancetrack(2).dll

Microsoft
contact Support
+1 888 851 3889 (Toll

Microsoft
Contact Support
+1-866-234-0420 (Toll Free)

Windows Security: Contact Support +1-866-234-0420 (Toll-Free)

Windows Defender Security Center

App: Ads.fiancetrack(2).dll
Threat Detected: Trojan Spyware

Windows was blocked due to questionable activity.
Contact Windows Support: 08 8121 8167 (Security Helpline)

Windows Security: Contact Support +61-1800-950-514 (Toll-Free)

Figure 1: Variety of fake virus popups

While very similar, the alerts feature different technical support phone numbers in Canada, the US, and Australia; text in English and French; and variations in phrasing, e.g., Toll-Free, Security Helpline.

Attack flow

A user browses their favorite publisher site to read the daily news or receive an update on hot celebrity gossip when they are presented a very simple, innocuous-looking ad [Figure 2]. Exclusive dinners and dog treats sound enticing, so they decide to click on the ad. The page redirects to a blog site, pklbogor[.]com that is basic in appearance and functionality [Figure 3].

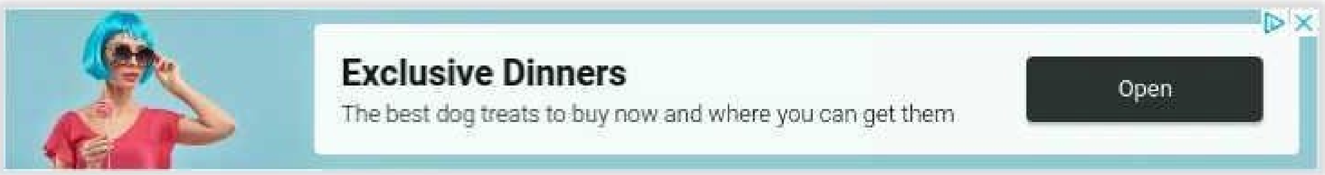
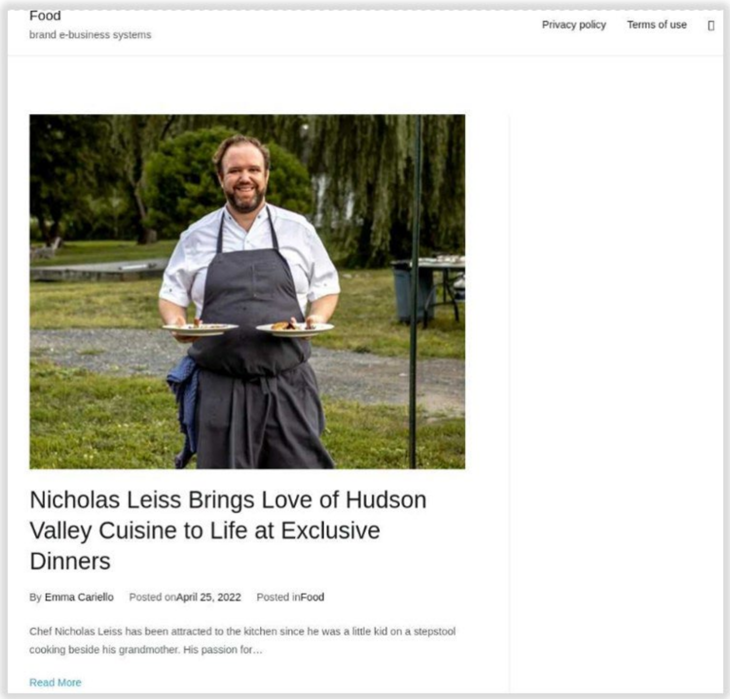


Figure 2: Creative for pklbogor[.]com



Nicholas Leiss Brings Love of Hudson Valley Cuisine to Life at Exclusive Dinners

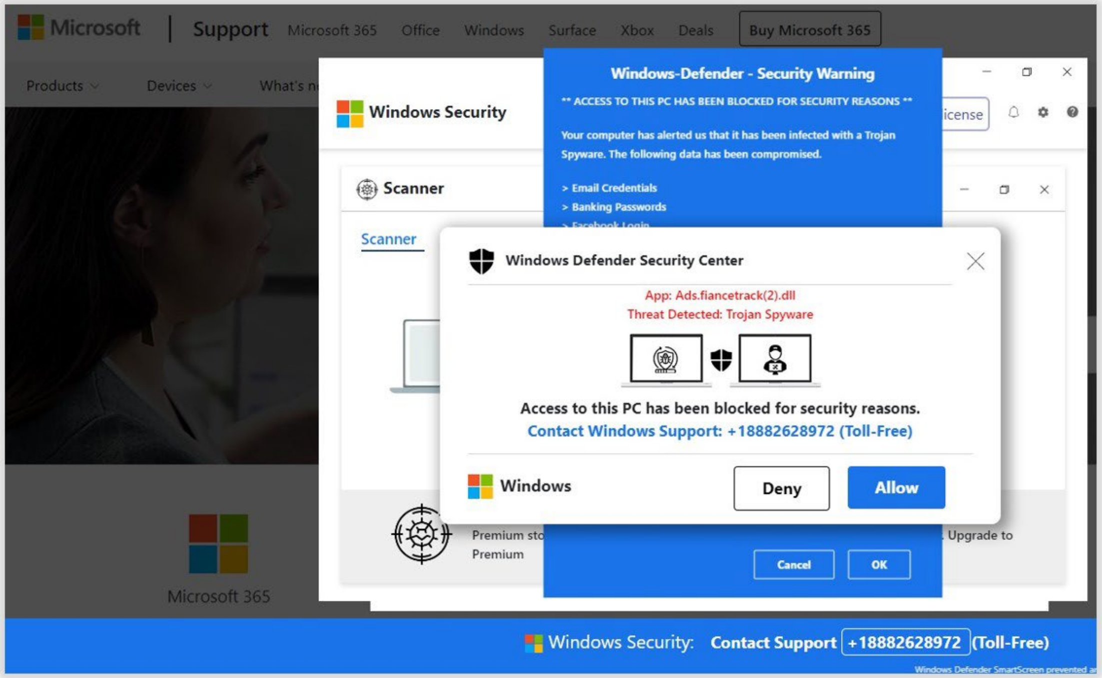
By Emma Cariello Posted onApril 25, 2022 Posted inFood

Chef Nicholas Leiss has been attracted to the kitchen since he was a little kid on a stepstool cooking beside his grandmother. His passion for...

Figure 3: Landing Page for creative in Figure 1 that resolves to pklbogor[.]com

Note that the landing page is a blog site with high-level, template-like content. The site contains about seven blog posts, and each post is about a hundred words long and does not contain much useful information.

However, there is something more sinister going on here. Given the right conditions, a user will instead be shown a landing page bombarded with multiple fake virus alerts. [Figure 4].



Windows-Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

> Email Credentials
> Banking Passwords
> Facebook Login

Windows Defender Security Center

App: Ads.fiancetrack(2).dll
Threat Detected: Trojan Spyware

Access to this PC has been blocked for security reasons.
Contact Windows Support: +18882628972 (Toll-Free)

Windows Security: Contact Support +18882628972 (Toll-Free)

Windows Defender SmartScreen prevented a

Figure 4: Fake virus alerts at pklbogor[.]com

Users are directed to contact the support number at the bottom of the page, which will eventually lead to the compromise of their device. In most instances the bad actor will offer to fix the device and remove the popup for a fee; however, the key objective is to gain access to the device and install backdoors for continued attacks,, e.g., ransomware, keyloggers, adware, spyware.

In order for the unsuspecting user to be redirected to this malicious content, the very simple following conditions must be met:

- Desktop
- Windows Operating System 7 & 10 (the most common), but likely others

As the malicious popups are Windows-based, the campaign checks for the victim's operating system. This increases the chances of appearing like a legitimate threat. However, the campaign has been confirmed to execute on Firefox, Chrome, and Chromium browsers. It's possible that this could affect iOS, but that has not been confirmed.

Deciphering the Pattern

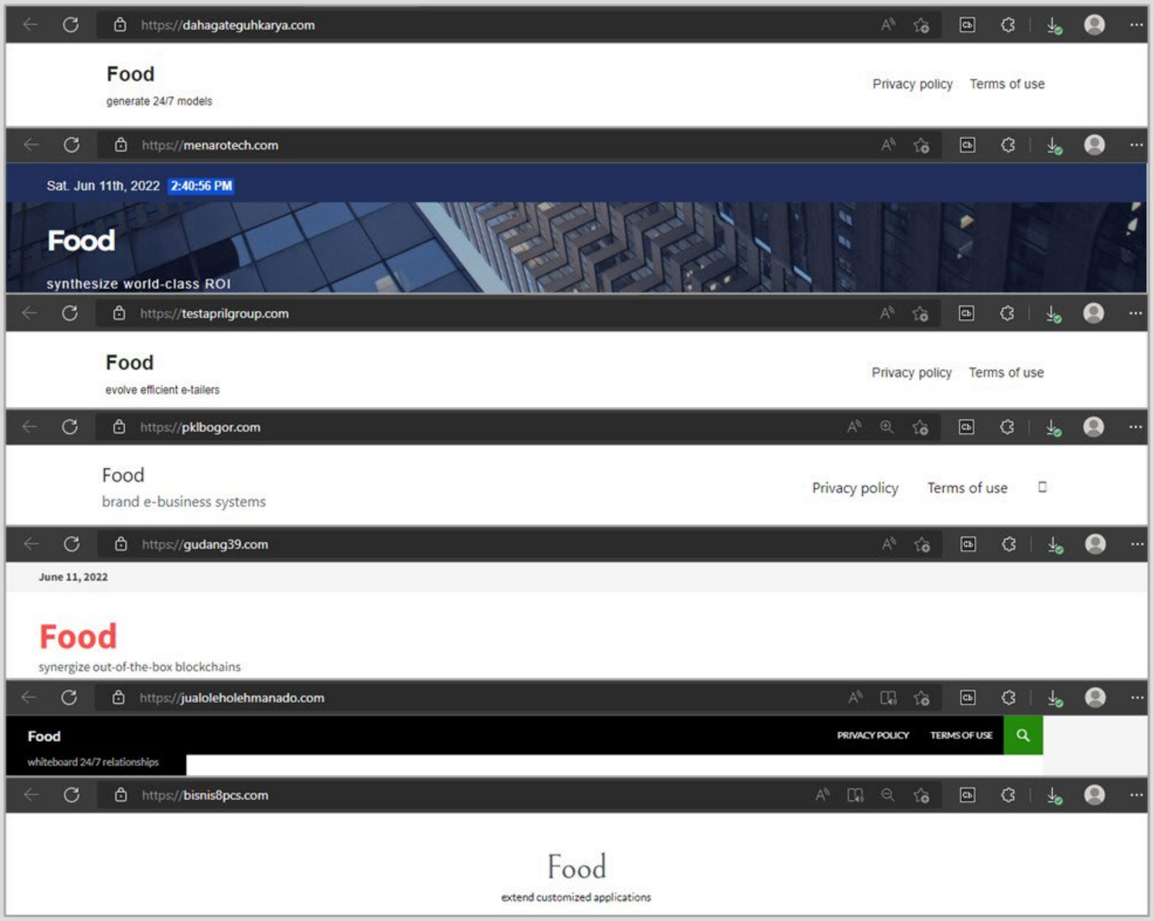
To broaden the reach of this campaign, bad actors will build a series of creative images and landing pages, requiring multiple domains. In addition to these domains being created and/or updated in a similar time period, the page structure will be similar.

The Dolos campaign uses three different cloaked landing page formats:

1. Fake: Basic, blog-like sites that contain minimal content and experience low site traffic; the domains were created and/or updated within days of each other
2. Generic: Sites have a more formal structure with navigation and contain seemingly more relevant information for the user; however, several links aren't operational and the content is frequently duplicated across multiple domains
3. Spoofed: Mimic the design, structure, and copy of legitimate brand websites.

CLOAKED LANDING PAGE FORMAT: FAKE

In Dolos, many of the cloaked malicious landing pages contain similar characteristics. In this particular instance, "food" is a common denominator, but there are signs that the pattern is being replicated with other keywords. [Figure 5] While additional keywords are not confirmed at this time, it is likely all part of the same evolving malicious campaign.



https://dahagateguhkarya.com

Food

generate 24/7 models

https://menarotech.com

Sat. Jun 11th, 2022 2:40:56 PM

Food

synthesize world-class ROI

https://testaprilgroup.com

Food

evolve efficient e-tailers

https://pklbogor.com

Food

brand e-business systems

https://gudang39.com

June 11, 2022

Food

synergize out-of-the-box blockchains

https://jualoleholehmanado.com

Food

whiteboard 24/7 relationships

https://bisnis8pcs.com

Food

extend customized applications

Figure 5: Generic blog sites with 'Food' in the header

Second, the image URLs on the landing page follow a similar format. For example,

- /wp-content/uploads/2022/03/thumb12.jpg
- /wp-content/uploads/2022/03/thumb14.jpg
- /wp-content/uploads/2022/03/thumb16.jpg
- /wp-content/uploads/2022/03/thumb17.jpg
- /wp-content/uploads/2022/03/thumb18.jpg

The presence of this URL pattern does not mean the page is malicious; however, its presence and other characteristics such as the generic, low-quality creative and landing page structure are good indications that this campaign requires additional analysis. Further investigation confirms the malicious activity—i.e., serving of multiple fake virus alerts on landing pages cloaked or hidden from initial analysis.

CLOAKED LANDING PAGE FORMAT: GENERIC

The second cloaked landing page format is a more legitimate looking blog site that will also lead to the fake virus alerts. Using similar—if not the same template—these domains are expressly created for the malicious campaign with most of the domains created and/or activated within days of campaign flight. In several instances the creative doesn't match the associated landing page. [Figure 6]

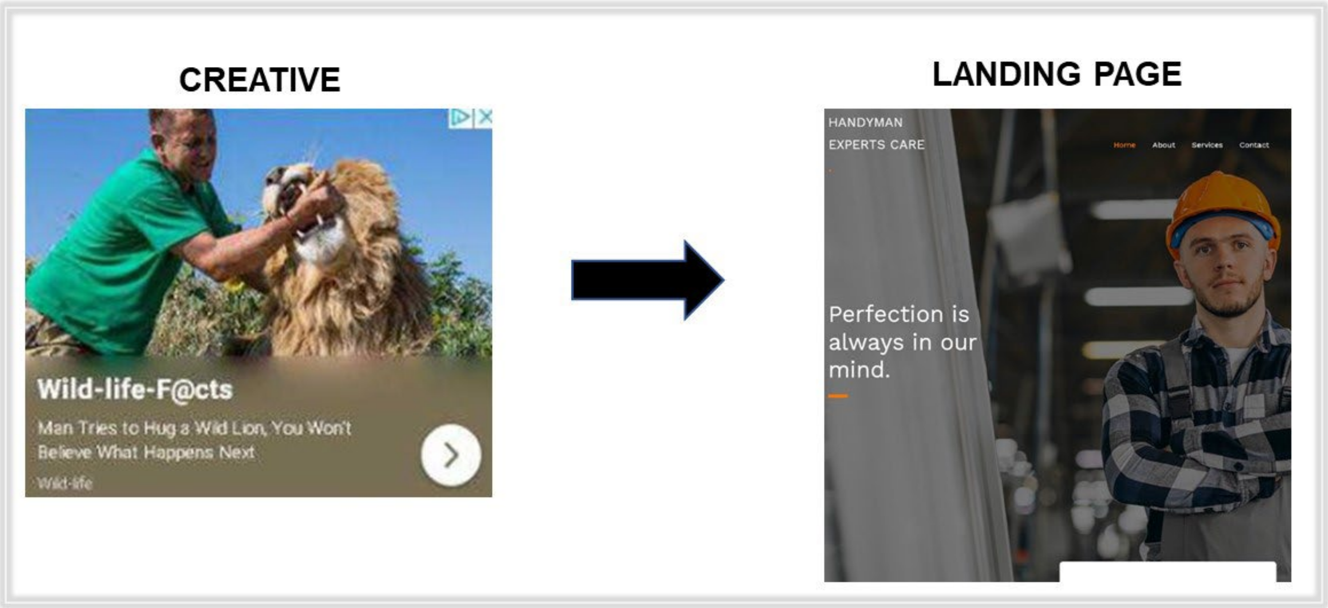

CREATIVE
Wild-life-F@cts
Man Tries to Hug a Wild Lion, You Won't Believe What Happens Next
Wild-life
LANDING PAGE
HANDYMAN EXPERTS CARE
Home
About
Services
Contact
Perfection is always in our mind.

Figure 6: Wildlife creative resolves to handymanexpertscare.com

Beyond the creative-landing page mismatch, the landing page appears as a legitimate advertiser promoting their business. Closer inspection reveals inactive links, duplicative content, and generic images. The same format is repeated over multiple domains. Again, if the correct conditions are met the visitor is served fake virus alerts instead of being directed to the associated landing page (handymanexpertscare[.]com).

CLOAKED LANDING PAGE FORMAT: SPOOFED

Spoof or mimic of a legitimate advertiser website is the third type of cloaked landing page format used by this threat actor. The spoofed page uses the same name, design, and content of a legitimate advertiser [Figure 7].

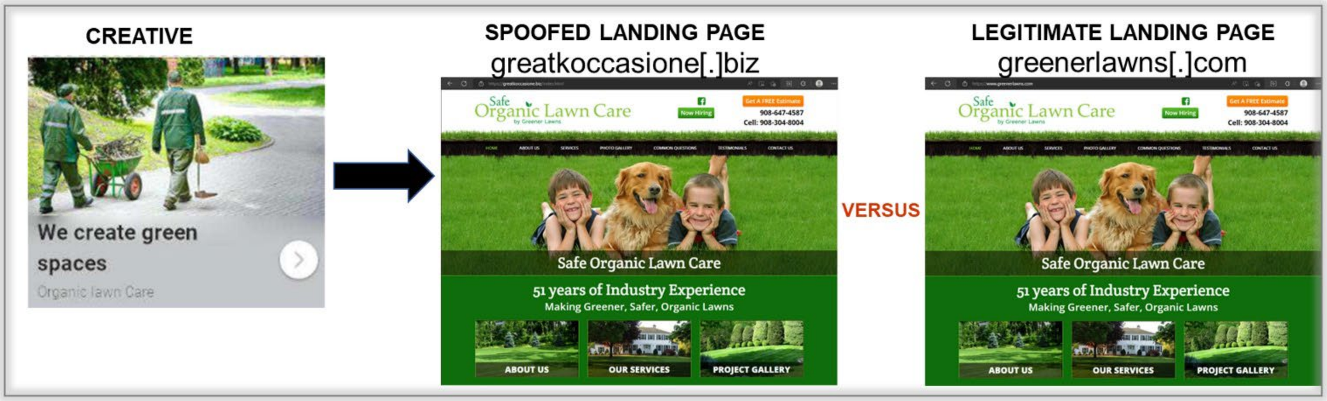


Figure 7: Comparison of greatkoccasione[.]biz spoofed site versus the legitimate greenerlawns[.]com

Even worse, in many instances only the URL top-level domain will be different. Sometimes, the site might contain rendering errors—e.g., iframe takes up the entire page creating issues with the scroll bars. [Figure 8]

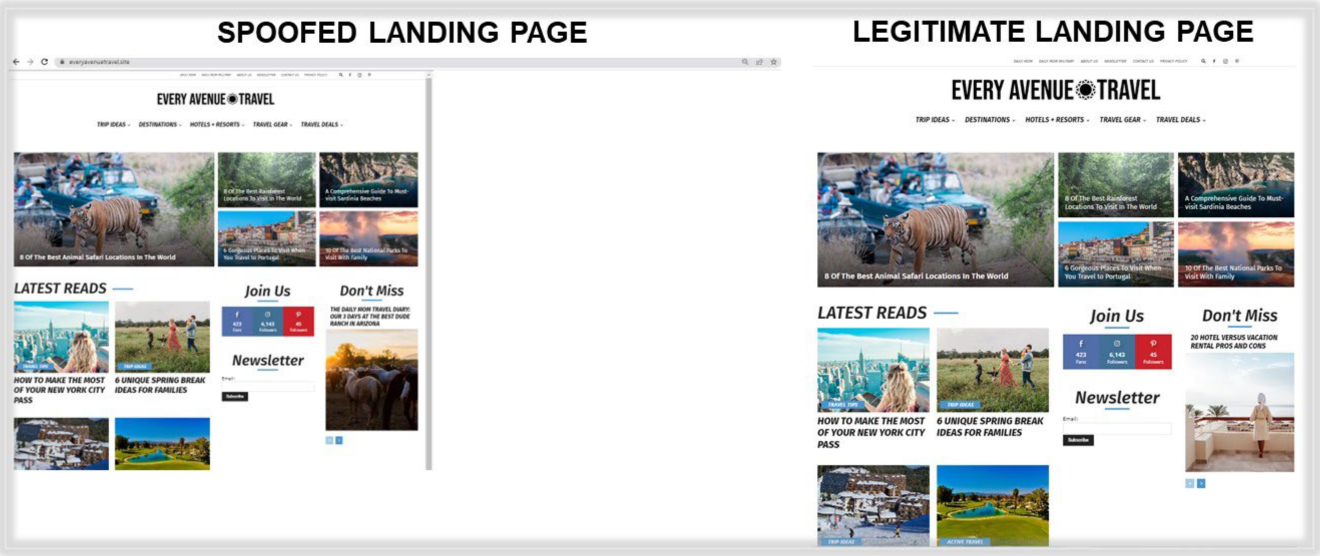


Figure 8: Comparison of everyavenuetravel[.]site spoofed site versus the legitimate everyavenuetravel[.]com

Rather than create their own content, malvertisers copy the landing page from an advertiser that is not well known. This makes it difficult to detect as searching for keywords from this page will generate legitimate results.

Despite the different attributes, the end result is the same. In all instances, if the correct conditions are met, users are directed to a landing page that serves the fake virus popups that lead to further compromise of the user’s device. [Figure 9]

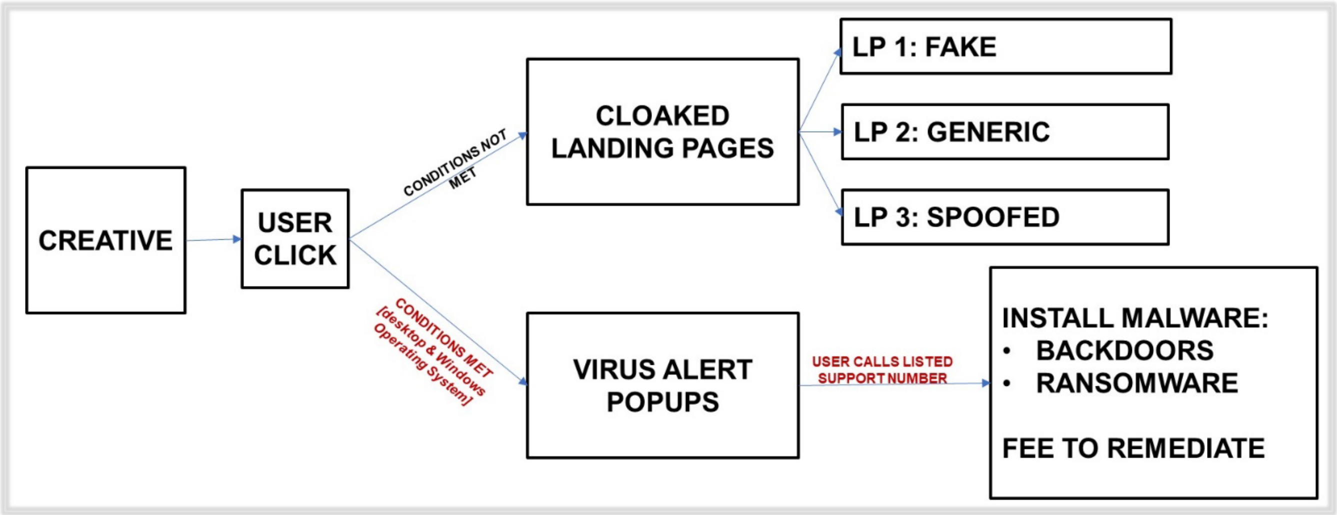


Figure 9: Attack flow for Dolos-3PC

Indicators of Compromise

These domains lead to malicious content that displays a popup window indicating that the user's device/machine may be infected, misleading them to believe they have a virus. This content can potentially manipulate the user into purchasing or installing a fake malware removal tool.

Fake Landing Page Domains that serve the malicious content
buzzhealthwire.info
handymanexpertscare.com
aranegf.com > redirects to d2pknlh4205hm8.cloudfront.net
delightvbored.biz
supertadmiralno.biz
letsmakethemsmiles.com
bestabureaucra.biz
trendrope.com
dahagateguhkarya.com
menarotech.com

testaprilgroup.com
pklbogor.com
gudang39.com
britishpropoliskids.com
jualoleholehmanado.com
bisnis8pcs.com
calderaproperty.com
start-hobbies.co.uk
grand-golf.co.uk
Everyavenuetravel.site > redirects to ‘whale-app-pu4yk.ondigitalocean.app’
greatkoccasione.biz
Thenextgenupdate.com > redirects to ‘idix.lol’
smartbedsalesgb. shop
safepcprotectionhelp.online
greatpsurgica.biz
bestoharcourtnc.biz
Mainlytrendy.com > redirects to ’orca-app-2-82gej.ondigitalocean.app’
superxembezzl.biz
thetimorlestepost.com
gudangblog.com

URLs hosting creative images and/or fake virus popups
s3.us-west-1.amazonaws.com/192.256.24.15.usa/winpop/index.html (called by safepcprotectionhelp.online)

s3.us-west-1.amazonaws.com/securityaccessblocked.25.24301145.15.com/winpop/index.html
s3.us-west-1.amazonaws.com/753.369.15.432.usa/pop/pop/script/index.html (called by buzzhealthwire.info)

Creatives

Though not exhaustive, these creatives—and various iterations and formats—are confirmed to be affiliated with the Dolos campaign. [Figure 10]

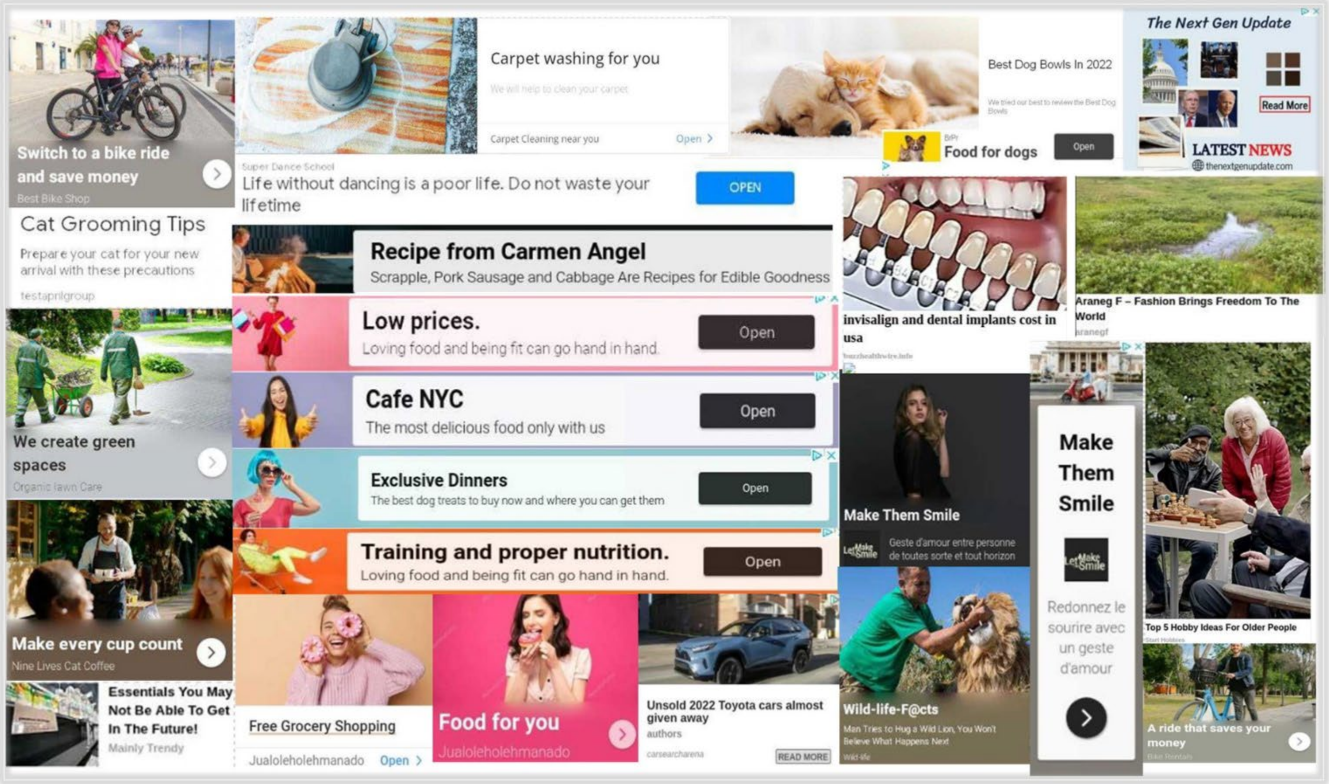

Switch to a bike ride and save money
Best Bike Shop
Carpet washing for you
We will help to clean your carpet
Carpet Cleaning near you
Open
Best Dog Bowls In 2022
Food for dogs
Open
The Next Gen Update
Read More
LATEST NEWS
thenextgenupdate.com
Cat Grooming Tips
Prepare your cat for your new arrival with these precautions
testapnlgroup
Super Dance School
Life without dancing is a poor life. Do not waste your lifetime
OPEN
Recipe from Carmen Angel
Scrapple, Pork Sausage and Cabbage Are Recipes for Edible Goodness
invisalign and dental implants cost in usa
Araneg F – Fashion Brings Freedom To The World
Low prices.
Loving food and being fit can go hand in hand.
Open
We create green spaces
Organic lawn Care
Cafe NYC
The most delicious food only with us
Open
Make Them Smile
Make Them Smile
Exclusive Dinners
The best dog treats to buy now and where you can get them
Open
Geste d'amour entre personne de toutes sorte et tout horizon
Training and proper nutrition.
Loving food and being fit can go hand in hand.
Open
Redonnez le sourire avec un geste d'amour
Make every cup count
Nine Lives Cat Coffee
Top 5 Hobby Ideas For Older People
Essentials You May Not Be Able To Get In The Future!
Mainly Trendy
Free Grocery Shopping
Jualoleholehmanado Open
Food for you
Jualoleholehmanado
Unsold 2022 Toyota cars almost given away
READ MORE
Wild-life-F@cts
Man Tries to Hug a Wild Lion, You Won't Believe What Happens Next
A ride that saves your money

Figure 10: Sampling of creative confirmed to be associated with cloaked landing pages

Impact

The resurgence of post-click malware requires continued analysis and vigilance. Since a late May uptick, The Media Trust has continued to identify cloaked landing pages leading to fake, Windows-based virus popups. Unsuspecting users—typically those lacking technological sophistication—fall into the trap and call the fake technical support number on the popups. Thinking that a support agent is on the line, they will be guided through various steps that lead to further compromise, such as the download of adware or remote access trojans. It is also common to see the malicious actors request money as a fee for the removal of the non-existent virus.

Although the victim will bear the consequences of falling for the scam, there are also consequences for the publisher serving these ads. If a user visiting a publisher site is regularly met with this type of malware, they will lose confidence in the publisher and their efforts to combat malicious ads, which will eventually depreciate inventory value. One or two people may not make a difference for the publisher but malicious campaigns are widespread and can affect thousands of unique visitors a day, and the numbers add up.

Actions to defend against Dolos-3PC

The success of these campaigns lies in the post-click malware delivery. The innocuous-looking creatives and tags will pass quality review. Stopping the campaign requires a comprehensive list of affected creatives and cloaked landing pages—a difficult thing to do when new assets are added daily.

AdTech platforms and publishers should employ multi-level scanning (creative, tag, clickthrough, landing page) with a variety of device profiles to identify Dolos in action and keep on top of the continuous asset cycling. This will help build a portfolio of creatives and landing pages—as well as patterns—that can be widely recognized and aid in shutting down this specific threat and ones like it.