



```
bidaidea@h-c0n2023:~$ sudo adduser rafa --ingroup bidaidea
Adding user `rafa`
Adding new user `rafa` (1001) with group `bidaidea`
Enter the new value, or press ENTER for the default
    Full Name []: Rafael Tenorio
    Rol []: DFIR & CTI Service Manager @ Bidaidea
    Email []: rafael.tenorio@bidaidea.com
    Other []: GCTI/GCFA/GCFE/GASF/CISM en más de 10 años en estas batallas,
involucrado en incidentes internacionales, analizando APTs, liderando equipos de
ciberinteligencia y construyendo CSIRT/CERT en operaciones, todo con familia y
aficiones.
```

```
bidaidea@h-c0n2023:~$ sudo adduser luise --ingroup bidaidea
Adding user `luise`
Adding new user `luise` (1002) with group `bidaidea`
Enter the new value, or press ENTER for the default
    Full Name []: Luis Enrique Sainz
    Rol []: Cybersecurity Principal analyst @ Bidaidea
    Email []: luis.sainz@bidaidea.com
    Other []: cerca 20 años de experiencia en el desarrollo y de admin, siendo
reservista voluntario en el MCCE y radioaficionado.
```

```
bidaidea@h-c0n2023:~$ whoami
rafa/luise
```


Camino a Super Bowl

Los playoff del *malware*



A photograph of a workspace featuring a laptop on a white desk. The laptop screen shows a code editor with syntax-highlighted code on a dark background. In the background, a larger monitor displays a webpage, and a small potted plant sits on the desk. A large, semi-transparent question mark is overlaid on the left side of the image.

¿Está infectado?



VS



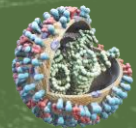
VS



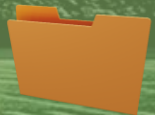
VS



VS



VS



VS



VS

VS

VS

VS

VS

```
bidaidea@h-c0n2023:~$ man funneling
```

NAME

Funneling

DESCRIPTION

1. Descartar lo conocido
2. Descartar lo NO dañino
3. Análisis del conjunto final

Wild Card

Divisional

Conference



VS

VS

VS

VS

```
bidaidea@h-c0n2023:~$ sudo ewfacquire -u -c "fast" -S "10GiB" -C "Playoff" -D  
"Dirty" -e "HeadCoach" -l /data/dirty/ewfacquire.log -t "/data/dirty/dirty"  
/dev/nvme0n1p3
```



```
caine@caine: ~  
File Edit View Search Terminal Help  
/dev/nvme0n1p2 206848 239615 32768 16M Microsoft reserved  
/dev/nvme0n1p3 239616 166729555 166489940 79,4G Microsoft basic data  
/dev/nvme0n1p4 166729728 167768063 1038336 507M Windows recovery environment  
  
Disk /dev/sda: 200 GiB, 214748364800 bytes, 419430400 sectors  
Disk model: VMware Virtual S  
Units: sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disklabel type: gpt  
Disk identifier: FBB2473F-C013-334A-8220-028499F90D5D  
  
Device Start End Sectors Size Type  
/dev/sda1 2048 419430366 419428319 200G Linux filesystem  
caine@caine:~$ sudo mount /dev/sda1 /mnt/  
caine@caine:~$ sudo umount /mnt  
caine@caine:~$ sudo mount /dev/sda1 /media/sda  
ntfs-3g-mount: failed to access mountpoint /media/sda: No such file or directory  
caine@caine:~$ sudo mount /dev/sda1 /mnt/  
caine@caine:~$ ls /mnt/  
clean dirty  
caine@caine:~$ sudo ewfacquire -u -c "fast" -S "10GiB" -C "Playoff" -D "Dirty" -  
e "HeadCoach" -l /mnt/dirty/log.txt -t "/mnt/dirty/dirty" /dev/nvme0n1p3
```

```
bidaidea@h-c0n2023:~$ sudo ewfmount /data/dirty/dirty.E01 /mnt/ewf_dirty
```

```
bidaidea@h-c0n2023:~$ sudo mount -t ntfs3 -o ro,loop /mnt/ewf_dirty/ewf1  
/mnt/windows02
```

```
bidaidea@h-c0n2023:~$ macrobber-ng -5 /mnt/windows02 > /data/dirty/dirty.body
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/dirty$ macrobber-ng -5 /mnt/windows02 > dirty.body  
jedi@eadu:/media/jedi/76FF193F32F8C57A/dirty$ ls -lh  
total 22G  
-rwxrwxrwx 1 jedi jedi 116M Feb  8 15:35 dirty.body  
-rwxrwxrwx 1 jedi jedi  10G Feb  8 10:36 dirty.E01  
-rwxrwxrwx 1 jedi jedi  10G Feb  8 10:46 dirty.E02  
-rwxrwxrwx 1 jedi jedi 1,2G Feb  8 10:54 dirty.E03  
-rwxrwxrwx 1 jedi jedi   65 Feb  8 10:54 log.txt  
jedi@eadu:/media/jedi/76FF193F32F8C57A/dirty$ head -n 3 dirty.body  
|/mnt/windows02/Documents and Settings|93524|lrwxrwxrwx -> /mnt/windows02/Users|0|0|20|1621348116.247863700|1621348116.247863700|  
1621348116.247863700|0.0  
0|/mnt/windows02/$Recycle.Bin|64|drwxrwxrwx|0|0|0|1675795731.536805400|1622619892.233908900|1622619892.233908900|0.0  
0|/mnt/windows02/$Recycle.Bin/S-1-5-18|100768|drwxrwxrwx|0|0|0|1622619892.233908900|1622619892.233908900|1622619892.233908900|0.0
```

Body file!!!!

MD5/Path/inodo/filetype+Permissions+linkfile/uid/gid/size/AMCB Time

Wild Card

Divisional

Conference



VS



VS

VS

VS

System Information



Operating System Version

Description

This determines the operating system type, version, build number and installation dates for current installation and previous updates.

Location

- SOFTWARE\Microsoft\Windows NT\CurrentVersion
- SYSTEM\Setup\Source OS

Interpretation

CurrentVersion key stores:

- **ProductName**, **EditionID** – OS type
- **DisplayVersion**, **ReleaseId**, **CurrentBuildNumber** – Version info
- **InstallTime** – Installation time of current build (not original installation)

Source OS keys are created for each historical OS update:

- **ProductName**, **EditionID** – OS type
- **BuildBranch**, **ReleaseId**, **CurrentBuildNumber** – Version info
- **InstallTime** – Installation time of this build version

- **Times present in names of Source OS keys are extraneous:**

InstallTime = 64-bit FILETIME format (Win10+)

InstallDate = Unix 32-bit epoch format

(both times should be equivalent)

Computer Name

Description

This stores the hostname of the system in the ComputerName value.

Location

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Interpretation

Hostname can facilitate correlation of log data and other artifacts.

System Boot & Autostart Programs

Description

System Boot and Autostart Programs, on system boot or at user login.

Location

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Autostart
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RunOnce
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- SYSTEM\CurrentControlSet\Services\IfStart value is set to 0x02, then service application (0x00 for drivers)

Interpretation

- Useful to find malware and to audit installed software
- This is not an exhaustive list of autorun locations

System Last Shutdown Time

Description

It is the last time the system was shutdown. On Windows XP, the number of shutdowns is also recorded.

Location

- SYSTEM\CurrentControlSet\Control\Windows (Shutdown Time)
- SYSTEM\CurrentControlSet\Control\Watchdog\Display (Shutdown Count – WinXP only)

Interpretation

- Determining last shutdown time can help to detect user behavior and system anomalies
- Windows 64-bit FILETIME format

SANS DFIR

FORENSICS & INCIDENT RESPONSE

Forensic Analyst

POSTER

- You Can't Protect the

[sics.sans.org](https://www.sans.org)


```
bidaidea@h-c0n2023:~$ rip.pl -r /mnt/dirty/Windows/System32/config/SOFTWARE -p winver
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/dirty$ rip.pl -r /mnt/dirty/Windows/System32/config/SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows 10 Home
ReleaseID             2009
BuildLab              19041.vb_release.191206-1406
BuildLabEx            19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID  Core
RegisteredOrganization
RegisteredOwner       Jedi
InstallDate           2021-05-18 14:28:41Z
InstallTime           2021-05-18 14:28:41Z
```

```
bidaidea@h-c0n2023:~$ rip.pl -r /mnt/dirty/Windows/System32/config/SYSTEM -p shutdown
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/dirty$ rip.pl -r /mnt/dirty/Windows/System32/config/SYSTEM -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2023-02-07 19:13:45Z
ShutdownTime : 2023-02-07 19:13:45Z
```

```
bidaiidea@h-c0n2023:~$ sudo ewfacquire -u -c "fast" -S "10GiB" -C "Playoff" -D  
"Clean" -e "HeadCoach" -l /data/clean/ewfacquire.log -t "/data/clean/clean"  
/dev/nvme0n1p3
```

```
-rwxrwxrwx 2 root root 18118 feb 7 19:45 DESKTOP-T6S1MS2-20230207-1945.log  
-rwxrwxrwx 1 root root 154320 feb 7 19:49 MpCmdRun.log  
-rwxrwxrwx 2 root root 1202 feb 7 19:49 MpCopyAccelerator.log  
-rwxrwxrwx 2 root root 407734 feb 7 19:49 MpSigStub.log  
drwxrwxrwx 1 root root 0 ott 22 2021 EdgeHeadache  
-rwxrwxrwx 2 root root 311692 ott 22 2021 msedge_installer.log  
-rwxrwxrwx 1 root root 262144 ott 22 2021 TS_273E.tmp  
-rwxrwxrwx 1 root root 196608 ott 22 2021 TS_520B.tmp  
-rwxrwxrwx 2 root root 1093632 set 9 2021 UpdHealthTools.msi  
drwxrwxrwx 1 root root 0 mag 18 2021 vmtoolsd-vmtoolsd  
-rwxrwxrwx 2 root root 78454 feb 7 19:50 vmware-vmtoolsd-SYSTEM.log  
-rwxrwxrwx 2 root root 1987 feb 7 19:42 vmware-vmtoolsd-Jedi.log  
-rwxrwxrwx 2 root root 1690 feb 7 19:42 vmware-vmtoolsd-SYSTEM.log  
-rwxrwxrwx 2 root root 37997 feb 7 19:50 vmware-vmtoolsd-Jedi.log  
-rwxrwxrwx 2 root root 1344 feb 7 19:38 vmware-vmtoolsd-SYSTEM.log  
drwxrwxrwx 1 root root 0 ott 22 2021 vmtoolsd  
caine@caine:~$ sudo umount /media/nvme0n1p  
/media/nvme0n1p1 /media/nvme0n1p3  
caine@caine:~$ sudo umount /media/nvme0n1p3  
caine@caine:~$ sudo umount /media/nvme0n1p1  
caine@caine:~$ sudo umount /mnt  
caine@caine:~$ ls /mnt/  
caine@caine:~$ sudo ewfacquire -u -c "fast" -S "10GiB" -C "Playoff" -D "Clean" -  
e "HeadCoach" -l /mnt/clean/log.txt -t "/mnt/clean/clean" /dev/nvme0n1p3
```

```
bidaiidea@h-c0n2023:~$ sudo ewfmount /data/clean/clean.E01 /mnt/ewf_clean  
bidaiidea@h-c0n2023:~$ sudo mount -t ntfs3 -o ro /mnt/ewf_clean /mnt/windows02  
bidaiidea@h-c0n2023:~$ macrobber-ng -5 /mnt/windows01 > /data/clean/clean.body
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/clean$ macrobber-ng -5 /mnt/windows01 > clean.body  
jedi@eadu:/media/jedi/76FF193F32F8C57A/clean$ ls -lh  
total 18G  
-rwxrwxrwx 1 jedi jedi 116M Feb 8 14:56 clean.body  
-rwxrwxrwx 1 jedi jedi 10G Feb 7 20:58 clean.E01  
-rwxrwxrwx 1 jedi jedi 7,5G Feb 7 21:11 clean.E02  
-rwxrwxrwx 1 jedi jedi 65 Feb 7 21:11 log.txt
```



```
bidaidea@h-c0n2023:~$ cd /wildcard
```

```
bidaidea@h-c0n2023:/wildcard$ cut -d '|' -f 1 dirty.body | sort | uniq > dirty_md5_uniqs.txt
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$ wc -l dirty_md5.txt
```

```
423257 dirty_md5.txt
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$ cut -d "|" -f 1 dirty.body | sort | uniq > dirty_uniqs_md5.txt
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$ wc -l dirty_uniqs_md5.txt
```

```
215827 dirty_uniqs_md5.txt
```

```
bidaidea@h-c0n2023:/wildcard$ for i in $(cat dirty_uniqs_md5.txt); do grep $i clean.body > /dev/null; if [ $? -gt 0 ] ; then echo $i >> md5_not_clean.txt; fi ; done
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$ for i in $(cat dirty_uniqs_md5.txt); do grep $i clean.body > /dev/null; if [ $? -gt 0 ] ; then echo $i >> md5_not_clean.txt; fi ; done
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$ wc -l md5_not_clean.txt
```

```
2924 md5_not_clean.txt
```

```
jedi@eadu:/media/jedi/76FF193F32F8C57A/wildcard$
```



Touchdown ! ! ! !

```

def body_parse(file, absolute_path, limit=10):
    """ This function returns a list of dicts with each file in the body file """
    files_object={}
    with open(file) as f:
        lines=0
        for line in f:
            fields=line[0:len(line)-1].split('|') #To remove the New Line
            if fields[0]==' ' or fields[0]==None or fields[0]=='0': # Remove empty lines and directories
                continue
            last_bar_pos=fields[1].rfind('/')+1
            filename=None
            extension=None
            if (last_bar_pos!=-1):
                filename=fields[1][last_bar_pos:]
                last_dot_pos=filename.rfind('.')+1
                extension=filename[last_dot_pos:]
                path=fields[1][len(absolute_path):last_bar_pos]
            else:
                path=fields[1][len(absolute_path):]
            file_obj={
                'md5': fields[0],
                'filename':filename,
                'extension':extension,
                'path': path,
                'size': int(fields[6]),
                'atime': float(fields[7]),
                'mtime': float(fields[8]),
                'ctime': float(fields[9]),
                'crttime': float(fields[10]),
            }
            files_object[file_obj['md5']]=file_obj
            if limit!=None and lines>limit:
                break
            lines=lines+1
    f.close()
    return files_object

```

```

def md5_list(file_list):
    md5_=set()
    i=0
    for file in file_list:
        md5_.add(file_list[file]['md5'])
        i=i+1
    return md5_

```

```

def list_compare(a, b):
    r=set()
    for e in a:
        if e not in b:
            r.add(e)
    return r

```



```
In [1]: ▶ import time
        from utilities import list_compare, md5_list, body_parse
```

```
In [2]: ▶ # Cargamos la lista de ficheros de la imagen limpia
        t1=time.time()
        files_clean=body_parse('../Data/clean/clean.body', '/mnt/windows01', None)
        md5_list_clean=md5_list(files_clean)
        t2=time.time()-t1
        print(("Cargados "+str(len(md5_list_clean))+ " ficheros en {:02.2f} segundos").format(t2))
```

Cargados 214740 ficheros en 0.93 segundos

```
In [3]: ▶ # Cargamos la lista de ficheros de la imagen sucia
        t1=time.time()
        files_dirty=body_parse('../Data/dirty/dirty.body', '/mnt/windows02', None)
        md5_list_dirty=md5_list(files_dirty)
        t2=time.time()-t1
        print(("Cargados "+str(len(md5_list_dirty))+ " ficheros en {:02.2f} segundos").format(t2))
```

Cargados 215825 ficheros en 0.90 segundos

```
In [4]: ▶ # Comparamos los sets
        files_difference=list_compare(md5_list_dirty, md5_list_clean)
        print("Hay " + str(len(files_difference)) + " ficheros diferentes")
```

Hay 2924 ficheros diferentes

Wild Card

Divisional

Conference



VS



VS



VS

VS



```
bidaidea@h-c0n2023:~$ cd /divisional
bidaidea@h-c0n2023:/divisional$ grep -f md5_not_clean.txt dirty.body > divisional.body
bidaidea@h-c0n2023:/divisional$ egrep
"\.exe\\|\\.dll\\|\\.msi\\|\\.vbs\\|\\.vbe\\|\\.bat\\|\\.ps1\\" divisional.body >
conference.body
```

```
jedi@eadu:/data/divisional$ egrep "\.exe\\|\\.dll\\|\\.msi\\|\\.vbs\\|\\.vbe\\|\\.bat\\|\\.ps1\\" divisional.body > conference.body
jedi@eadu:/data/divisional$ wc -l conference.body
602 conference.body
```

```
8ceclaf925f69f30a17f772b14662bca|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/mip_protection_sdk.dll|3
3cfa0341aa269dd8781e66614d94d9d5|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/loop_client.dll|39927
12f546eb0fd220609e2d4747e48aacc|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_bho.dll|3
cade8c94b6f83d98c949e2a8e078243d|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_bho_64.dll|3
70e19e4a1b095398fb044cdb0a8a8150|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_stub.exe|3
008ad741e745236b2cc546999966726c|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-sysinfo-l1-1-0.dll|125933|-
d1f061c3ceb4f6af11f5e3c174507573|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-timezone-l1-1-0.dll|125106|-
fd1ffb1bcf3315dade9842baa522e2ed|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-util-l1-1-0.dll|125897|-rwx
a226a2c9dba8ba379bc46f0ecd270669|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-crt-conio-l1-1-0.dll|125949|-rwx
a25b00fc770046028282a18cccc002a15|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-crt-convert-l1-1-0.dll|126020|-
```

```
bidaidea@h-c0n2023:/divisional$ egrep -v
"/Program Files \(x86\)\\Microsoft\\Edge|\\Users\\.*\\AppData\\Local\\Microsoft\\Teams"
conference.body > conference_Extratime.body
```

```
jedi@eadu:/data/divisional$ egrep -v "/Program Files \(x86\)\\Microsoft\\Edge|\\Users\\.*\\AppData\\Local\\Microsoft\\Teams"
conference.body > conference_Extratime.body
jedi@eadu:/data/divisional$ wc -l conference_Extratime.body
13 conference_Extratime.body
```



```
bidaidea@h-c0n2023:~$ cd /divisional
bidaidea@h-c0n2023:/divisional$ grep -f md5_not_clean.txt dirty.body > divisional.body
bidaidea@h-c0n2023:/divisional$ egrep
"\.exe\\|\\.dll\\|\\.msi\\|\\.vbs\\|\\.vbe\\|\\.bat\\|\\.ps1\\|" divisional.body >
conference.body
```

```
jedi@eadu:/data/divisional$ egrep "\.exe\\|\\.dll\\|\\.msi\\|\\.vbs\\|\\.vbe\\|\\.bat\\|\\.ps1\\|" divisional.body > conference.body
jedi@eadu:/data/divisional$ wc -l conference.body
602 conference.body
```

```
8ceclaf925f69f30a17f772b14662bca|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/mip_protection_sdk.dll|3
3cfa0341aa269dd8781e66614d94d9d5|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/loop_client.dll|39927
12f546eb0fd220609e2d4747e48aacc|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_bho.dll|3
cade8c94b6f83d98c949e2a8e078243d|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_bho_64.dl
70e19e4a1b095398fb044cdb0a8a8150|/mnt/windows02/Program Files (x86)/Microsoft/Edge/Application/109.0.1518.78/BHO/ie_to_edge_stub.exe|
008ad741e745236b2cc546999966726c|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-sysinfo-l1-1-0.dll|125933|
d1f061c3ceb4f6af11f5e3c174507573|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-timezone-l1-1-0.dll|125106|
fd1ffb1bcf3315dade9842baa522e2ed|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-core-util-l1-1-0.dll|125897|-rwx
a226a2c9dba8ba379bc46f0ecd270669|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-crt-conio-l1-1-0.dll|125949|-rwx
25b00fc770046020202a10cccc002a15|/mnt/windows02/Users/Jedi/AppData/Local/Microsoft/Teams/current/api-ms-win-crt-convert-l1-1-0.dll|126020|
```

```
bidaidea@h-c0n2023:/divisional$ egrep -v
"/Program Files \(x86\)\\Microsoft\\Edge|\\Users\\.*\\AppData\\Local\\Microsoft\\Teams"
conference.body > conference_Extratime.body
```

```
jedi@eadu:/data/divisional$ egrep -v "/Program Files \(x86\)\\Microsoft\\Edge|\\Users\\.*\\AppData\\Local\\Microsoft\\Teams"
conference.body > conference_Extratime.body
jedi@eadu:/data/divisional$ wc -l conference_Extratime.body
13 conference_Extratime.body
```



Touchdown!!!!

```
In [5]: ► print("Filtramos por extensión...")
interesting_extensions={'exe', 'dll', 'msi', 'bat', 'ps1', 'vbs', 'vbe'}
cleanup_set=set()
for file_md5 in files_difference:
    extension=files_dirty[file_md5]['extension'].lower()
    if (extension not in interesting_extensions):
        cleanup_set.add(file_md5)
print("\tQuitando "+str(len(cleanup_set))+ " elementos")
for e in cleanup_set:
    files_difference.remove(e)
```

```
Filtramos por extensión...
    Quitando 2570 elementos
```

[illegible]


```
In [6]: ► print("Limpiando por rutas...")
exclude_paths=["\\Program Files \\(x86\\)\\Microsoft\\Edge",
               "\\Users\\[a-zA-Z0-9]+\\AppData\\Local\\Microsoft\\Teams",]
for path in exclude_paths:
    print("\tPath filter: "+path)
    cleanup_set=set()
    pattern = re.compile(path)
    for file_md5 in files_difference:
        if pattern.match(files_dirty[file_md5]['path']):
            cleanup_set.add(file_md5)
    print("\t\tQuitando "+str(len(cleanup_set))+ " elementos")
    for e in cleanup_set:
        files_difference.remove(e)
```

Limpiando por rutas...

Path filter: \\Program Files \\(x86\\)\\Microsoft\\Edge

Quitando 152 elementos

Path filter: \\Users\\[a-zA-Z0-9]+\\AppData\\Local\\Microsoft\\Teams

Quitando 190 elementos

Wild Card



VS



Divisional



VS



Conference



VS



VS

```
bidaidea@h-c0n2023:~$ cd /conference
bidaidea@h-c0n2023:/conference$ cut -d "|" -f 1 conference_Extratime.body >
conference_hashes.txt
bidaidea@h-c0n2023:~$ cat conference_hashes.txt
1f083f5a820468e5438c32419525b798
c1146dfa30d3bce2f4ee6f5282786e3a
50de124907b4e6aa5adba60f9cc22ed0
0ee2b50c85a110689352fccfa77b5b18
50de124907b4e6aa5adba60f9cc22ed0
c18b690c9f7cf921d35d97e87766b209
cb8020836e77353f5229fe43d436e386
97cf870f1d1fdc83640e3c8d8ec81c66
fdb53152230e3beafccbc2aaf2a00165
370b191519abcd3956a065bb89eb9445
6a49ba414d53c304bddcbd4a501281cd
cf7dc712c6b4fff1107f28f9bdac829b
aeca0aa59566b054ca9283cfc33e45a4
```


aeca0aa5c56c1954e0000500454

ThreatPinch Bulk Lookups | Perform lookups on lists of observables

<input checked="" type="checkbox"/>	1f083f5a820468e5438c32419525b798
<input checked="" type="checkbox"/>	c1146dfa30d3bce2f4ee6f5282786e3a
<input checked="" type="checkbox"/>	50de124907b4e6aa5adba60f9cc22ed0
<input checked="" type="checkbox"/>	0ee2b50c85a110689352fccfa77b5b18

ThreatPinch Bulk Lookups | Perform lookups on lists of observables

Settings | Customize

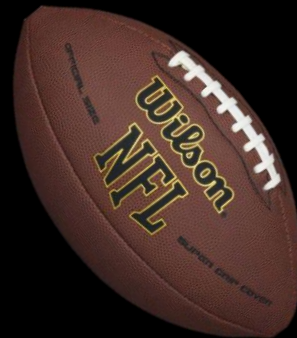
API Limit (in seconds):

Website Emulation (For Filtering):

Show All Pivots: ☐ Show Graph: ☒

Lookup List | Paste list here

1f083f5a820468e5438c32419525b798
c1146dfa30d3bce2f4ee6f5282786e3a
50de124907b4e6aa5adba60f9cc22ed0
0ee2b50c85a110689352fccfa77b5b18
50de124907b4e6aa5adba60f9cc22ed0
c18b690c9f7cf921d35d97e87766b209
cb8020836e77353f5229fe43d436e386
97cf870f1d1fdc83640e3c8d8ec81c66
fdb53152230e3beafccbc2aaf2a00165
370b191519abcd3956a065bb89eb9445
6a49ba414d53c304bddcbd4a501281cd
cf7dc712c6b4fff1107f28f9bdac829b
aeca0aa59566b054ca9283cfc33e45a4



Touchdown ! ! ! !

```
def check_hash_bazaar(hash):  
    """Checks a hash against the Malware Bazaar Database"""  
    cached=cache.get('mb', hash)  
    if cached is None:  
        url="https://mb-api.abuse.ch/api/v1/"  
        r = requests.post(url, data={'query':'get_info', 'hash':hash})  
        if (r.status_code==404):  
            cached={  
                'is_known': 0,  
            }  
        elif (r.status_code==200):  
            res=r.json()  
            if res["query_status"]=="hash_not_found":  
                cached={  
                    'is_known': 0,  
                }  
            elif res["query_status"]=="ok":  
                cached={  
                    'is_known': 1,  
                    'extra': res  
                }  
            cache.set('mb', hash, cached)  
    return cached
```



```
def capev2_check(hash, cape_url):
    cape_api_url=cape_url+'/apiv2'
    r = requests.get(cape_api_url+'/tasks/search/md5/'+hash)
    if (r.status_code==404):
        print("\nSomething failed communicating with CAPE")
        return None
    else:
        tasks=r.json()['data']
        if len(tasks)==0:
            return False
        res={
            'score': 0,
            'detections': []
        }
        print("CAPEv2 findings for "+hash+":")
        for task in tasks:
            cape_api_url+'/tasks/get/report/'+str(task['id'])
            if task['status']=="reported":
                q = requests.get(cape_api_url+'/tasks/get/report/'+str(task['id']))
                if (q.status_code==200):
                    report=q.json()
                    print('\t target:'+task['target']+ ' ['+task['category']+'] score: '+str(report['malscore'])+'/10 -> "+cape_url+'/analysis/'+str(task['id'])+'/'')
                    res['score']=res['score']+report['malscore']
                    if 'detections' in report:
                        res['detections'].append(report['detections'])
            elif task['status']=="running" or task['status']=="reporting" or task['status']=="pending":
                return True
        res['score']=res['score']/len(tasks)
        return res
```

```

def capev2_check(hash, cape_url):
    cape_api_url=cape_url+'/apiv2'
    r = requests.get(cape_api_url+'/tasks/search/md5/'+hash)
    if (r.status_code==404):
        print("\nSomething failed communi
        return None
    else:
        tasks=r.json()['data']
        if len(tasks)==0:
            return False
        res={
            'score': 0,
            'detections': []
        }
        print("CAPEv2 findings for "+hash)
        for task in tasks:
            cape_api_url+'/tasks/get/repo
            if task['status']=="reported"
                q = requests.get(cape_api
                if (q.status_code==200):
                    report=q.json()
                    print('\t target: '+ta
                    res['score']=res['sco
                    if 'detections' in re
                        res['detections']
                elif task['status']=="running
                    return True
        res['score']=res['score']/len(tasks)
        return res

def check_hash_circllu(hash):
    """Checks a hash against de circl.lu known files database"""
    cached=cache.get('circllu', hash)
    if cached is None:
        url="https://hashlookup.circl.lu/lookup/md5/%s" % (hash)
        r = requests.get(url)
        if (r.status_code==404):
            cached={
                'is_known': 0,
            }
        elif (r.status_code==200):
            res=r.json()
            cached={
                'is_known': 1,
                'extra': res
            }
        cache.set('circllu', hash, cached)
    return cached

e_url+'/analysis/'+str(task['id'])+ '/'')

```

```

def capev2_check(hash,
    cape_api_url=cape_u
    r = requests.get(cape
    if (r.status_code==
        print("\nSometh
        return None
    else:
        tasks=r.json()[
        if len(tasks)==
            return Fals
        res={
            'score': 0,
            'detections
        }
        print("CAPEv2 f
        for task in tas
            cape_api_ur
            if task['st
                q = req
                if (q.s
                    rep
                    pri
                    res
                    if
                elif task['
                    return
            res['score']=re
            return res

```

```

def check_hash_ms(hash: str, MS_API: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('ms', hash)
    if cached is None:
        url="https://malshare.com/api.php?api_key=%s&action=details&hash=%s" % (MS_API, hash)
        r = requests.post(url)
        res=r.json()
        if len(res)>0:
            if 'ERROR' in res:
                if res['ERROR']['CODE']==404:
                    cached={
                        'is_malware': 0,
                        'extra': res
                    }
                else:
                    print("U0")
            else:
                cached={
                    'is_malware': 1,
                    'extra': res
                }
            else:
                cached={
                    'is_malware': 0
                }
            cache.set('ms', hash, cached)
        return cached

```

+str(task['id'])+ '/')


```

def check_hash_ms(hash: str, MS_API: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('ms', hash)
    if cached is None:
        url="https://malshare.com/api.php?api_key=%s&action=details&hash=%s" % (MS_API, hash)

def capev2_check(hash,
    cape_api_url=cape_u
    r = requests.get(cape
    if (r.status_code==

def check_hash_vt(hash: str, VT_API: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('vt', hash)
    if cached is None:
        client = vt.Client(VT_API)
        file = client.get_object("/files/"+hash)
        if (file.last_analysis_stats['undetected']+file.last_analysis_stats['harmless'])>0:
            is_virus=(file.last_analysis_stats['malicious']+file.last_analysis_stats['suspicious'])/(file.last_analysis_stats['undetected']+file.last_analysis_stats['harmless'])
        else:
            is_virus=(file.last_analysis_stats['malicious']+file.last_analysis_stats['suspicious'])
        cached={
            'is_malware': is_virus>1,
            'extra': {
                'undetected': file.last_analysis_stats['undetected'],
                'malicious': file.last_analysis_stats['malicious'],
                'suspicious': file.last_analysis_stats['suspicious'],
                'harmless': file.last_analysis_stats['harmless'],
            }
        }
        print(hash, cached)
        cache.set('vt', hash, cached)
        sleep(15) #TODO: implementar throttling de verdad
    return cached

    elif task[
        return
    res['score']=re
    return res

        cached={
            'is_malware': 0
        }
        cache.set('ms', hash, cached)
    return cached

```

```

def check_hash_ms(hash: str, MS_API: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('ms', hash)
    if cached is None:
        url='https://www.virustotal.com/api/v3/analyses/'+hash
        r = requests.get(url)
        if (r.status_code==200):
            result=r.json()
            res['score']=result['score']
            return res
        else:
            return None
    cache.set('ms', hash, cached)
    return cached

def capev2_check(hash: str, cape_api_url: str):
    """Receives a hash and returns an object with the result"""
    url=cape_api_url+hash
    r = requests.get(url)
    if (r.status_code==200):
        result=r.json()
        res['score']=result['score']
        return res
    else:
        return None

def check_hash_vt(hash: str, VT_API: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('vt', hash)
    if cached is None:
        client = vt.Client(VT_API)
        file = client.get_object("/files/"+hash)
        if (file.last_analysis_stats['undetected'] > 0):
            is_virus=(file.last_analysis_stats['undetected'] > 0)
        else:
            is_virus=(file.last_analysis_stats['malicious'] > 0)
        cached={
            'is_malware': is_virus>1,
            'extra': {
                'undetected': file.last_analysis_stats['undetected'],
                'malicious': file.last_analysis_stats['malicious'],
                'suspicious': file.last_analysis_stats['suspicious'],
                'harmless': file.last_analysis_stats['harmless']
            }
        }
        print(hash, cached)
        cache.set('vt', hash, cached)
        sleep(15) #TODO: implementar throttling de verdad
    return cached

def check_hash_alienvault(hash: str, key: str):
    """Receives a hash and returns an object with the result"""
    cached=cache.get('alienvault', hash)
    if cached is None:
        otx = OTXv2(key)
        result=otx.file(hash)
        if len(result) > 0:
            print('Identified as potentially malicious')
            #print(str(result))
            cached={
                'is_malware': 1
            }
        else:
            #print('Unknown or not identified as malicious')
            cached={
                'is_malware': 0
            }
        cache.set('alienvault', hash, cached)
        #sleep(15) #TODO: implementar throttling de verdad
    return cached

```



```
pidgenx.dll -> application/x-dosexec [OK]
Microsoft.CognitiveServices.Speech.core.dll -> application/x-dosexec [OK]
expressrip.exe -> application/x-dosexec [OK]
Installer.exe -> application/x-dosexec [OK]
msvcp120.dll -> application/x-dosexec [OK]
combase.exe -> application/x-dosexec [OK]
mp3enc.exe -> application/x-dosexec [OK]
PDFPower.exe -> application/x-dosexec [OK]
KeyCheck.exe -> application/x-dosexec [OK]
KInfo.exe -> application/x-dosexec [OK]
ripsetup.exe -> application/x-dosexec [OK]
msvcr120.dll -> application/x-dosexec [OK]
```

MD5	Fichero	VT	MalShare	AlienWare OTX	MalwareBazaar	CAPEv2	ClamAv	Malware Hash Registry	MISP	Circl.lu
fdb53152230e3beafcdbc2aaf2a00165	pidgenx.dll	0/69	-	0	-	1.3/10	-	0%	-	Conocido (que no seguro)
cf7dc712c6b4fff1107f28f9bdac829b	ripsetup.exe	0/72	-	0	-	8.5/10	-	0%	-	-
97cf870f1d1fdc83640e3c8d8ec81c66	msvcr120.dll	0/65	-	0	-	1.6/10	-	0%	-	-
c18b690c9f7cf921d35d97e87766b209	KInfo.exe	0/56	-	0	-	0.4/10	-	0%	-	-
aeca0aa59566b054ca9283cfc33e45a4	combase.exe	55/71	-	0	X	5.9/10	-	17%	-	-
cb8020836e77353f5229fe43d436e386	msvcpr120.dll	0/69	-	0	-	1.6/10	-	0%	-	-
50de124907b4e6aa5adba60f9cc22ed0	Installer.exe	3/68	-	0	-	10/10	-	0%	-	-
1f083f5a820468e5438c32419525b798	mp3enc.exe	2/68	-	0	-	1.1/10	-	0%	-	-
370b191519abcd3956a065bb89eb9445	KeyCheck.exe	23/45	-	0	-	7.2/10	-	0%	-	-
0ee2b50c85a110689352fccfa77b5b18	Microsoft.CognitiveServices.Speech.core.dll	0/69	-	0	-	-	-	0%	-	Conocido (que no seguro)
6a49ba414d53c304bddcbd4a501281cd	PDFPower.exe	0/70	-	0	-	3.6/10	-	0%	-	-
c1146dfa30d3bce2f4ee6f5282786e3a	expressrip.exe	2/64	-	0	-	6.1/10	-	0%	-	-

Wild Card



VS



Divisional



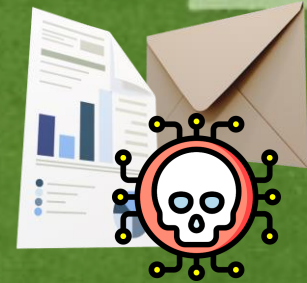
VS



Conference



VS



VS




```
bidaidea@h-c0n2023:~$ cd /superbowl
```

```
bidaidea@h-c0n2023:/superbowl$ cat superbowl.body
```

```
jedi@eadu:/data/superbowl$ cat superbowl.body
```

```
1f083f5a820468e5438c32419525b798|/mnt/windows02/Program Files (x86)/NCH Software/Components/mp3el/mp3enc.exe|398931|  
c1146dfa30d3bce2f4ee6f5282786e3a|/mnt/windows02/Program Files (x86)/NCH Software/ExpressRip/expressrip.exe|398921|-r  
50de124907b4e6aa5adba60f9cc22ed0|/mnt/windows02/Program Files (x86)/NCH Software/ExpressRip/expressripsetup_v5.00.ex  
50de124907b4e6aa5adba60f9cc22ed0|/mnt/windows02/Users/Jedi/AppData/Local/Temp/ExpressRip-9004-1/Installer.exe|398912  
370b191519abcd3956a065bb89eb9445|/mnt/windows02/Users/Jedi/Documents/KeyCheck v1.0.3.6_RU_EN_ES_VI_LV/KeyCheck.exe|3  
aeca0aa59566b054ca9283cfc33e45a4|/mnt/windows02/Windows/Temp/combase.exe|235858|-rwxrwxrwx|0|0|804352|1675797199.806
```

```
bidaidea@h-c0n2023:/superbowl$ mactime -b superbowl.body > superbowl.MACBtime.txt
```

```
bidaidea@h-c0n2023:/superbowl$ cat superbowl.MACBtime.txt
```

```
jedi@eadu:/data/superbowl$ mactime -b superbowl.body > superbowl.MACBtime.txt
```

```
jedi@eadu:/data/superbowl$ cat superbowl.MACBtime.txt
```

Tue May 06 2014 09:07:36	315904	...b	-rwxr-xr-x	0	0	399830	/mnt/windows01/Users/Jedi/Documents/KeyCheck v1.0.3.6_RU_EN_ES_VI_LV/KeyCheck.exe
Tue Feb 08 2022 17:37:32	1111568	m...	-rwxr-xr-x	0	0	398921	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressrip.exe
Tue Feb 07 2023 19:11:06	804352	m...	-rwxr-xr-x	0	0	235858	/mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 19:56:03	607760	...b	-rwxr-xr-x	0	0	398912	/mnt/windows01/Users/Jedi/AppData/Local/Temp/ExpressRip-9004-1/Installer.exe
Tue Feb 07 2023 19:56:04	607760	m.c.	-rwxr-xr-x	0	0	398912	/mnt/windows01/Users/Jedi/AppData/Local/Temp/ExpressRip-9004-1/Installer.exe
	607760	m.c.	-rwxr-xr-x	0	0	398965	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressripsetup_v5.00.exe
Tue Feb 07 2023 19:56:17	1111568	..cb	-rwxr-xr-x	0	0	398921	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressrip.exe
Tue Feb 07 2023 19:56:18	110592	macb	-rwxr-xr-x	0	0	398931	/mnt/windows01/Program Files (x86)/NCH Software/Components/mp3el/mp3enc.exe
Tue Feb 07 2023 19:56:21	607760	.a..	-rwxr-xr-x	0	0	398912	/mnt/windows01/Users/Jedi/AppData/Local/Temp/ExpressRip-9004-1/Installer.exe
	607760	...b	-rwxr-xr-x	0	0	398965	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressripsetup_v5.00.exe
Tue Feb 07 2023 19:56:22	607760	.a..	-rwxr-xr-x	0	0	398965	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressripsetup_v5.00.exe
Tue Feb 07 2023 20:06:50	1111568	.a..	-rwxr-xr-x	0	0	398921	/mnt/windows01/Program Files (x86)/NCH Software/ExpressRip/expressrip.exe
Tue Feb 07 2023 20:07:04	315904	m...	-rwxr-xr-x	0	0	399830	/mnt/windows01/Users/Jedi/Documents/KeyCheck v1.0.3.6_RU_EN_ES_VI_LV/KeyCheck.exe
Tue Feb 07 2023 20:07:19	315904	..c.	-rwxr-xr-x	0	0	399830	/mnt/windows01/Users/Jedi/Documents/KeyCheck v1.0.3.6_RU_EN_ES_VI_LV/KeyCheck.exe
Tue Feb 07 2023 20:07:33	315904	.a..	-rwxr-xr-x	0	0	399830	/mnt/windows01/Users/Jedi/Documents/KeyCheck v1.0.3.6_RU_EN_ES_VI_LV/KeyCheck.exe
Tue Feb 07 2023 20:11:38	804352	...b	-rwxr-xr-x	0	0	235858	/mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 20:13:03	804352	..c.	-rwxr-xr-x	0	0	235858	/mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 20:13:19	804352	.a..	-rwxr-xr-x	0	0	235858	/mnt/windows01/Windows/Temp/combase.exe



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows® Time Rules¹

\$Standard_Information Win10 v1903



File Creation

Modified –
Time of File
Creation

Access –
Time of
File Creation

Metadata –

File Access

Modified –
No Change

Access –
Time of Access
(No Change If System
Volume > 128 GiB)

Metadata –

File Modification

Modified –
Time of Data
Modification

Access –
Time of Data
Modification

Metadata –

File Rename

Modified –
No Change

Access –
No Change

Metadata –

File Copy (new file)

Modified –
Inherited
from Original

Access –
Time of
File Copy

Metadata –

Local File Move

Modified –
No Change

Access –
No Change

Metadata –

Volume File Move (move via CLI)

Modified –
Inherited
from Original

Access –
Time of File
Move via CLI

Metadata –

Volume File Move (cut/paste via Explorer)

Modified –
Inherited
from Original

Access –
Time of
Cut/Paste

Metadata –

File Deletion (shift+delete)

Modified –
No Change

Access –
No Change

Metadata –

17b6e0bb426b762e1caee67606532e3350d8c752c0625994424916e0fba527ab



?

Community Score

55 security vendors and 3 sandboxes flagged this file as malicious

17b6e0bb426b762e1caee67606532e3350d8c752c0625994424916e0fba527ab

wFCW.exe

peexe

assembly

runtime-modules

detect-debug-environment

checks-network-adapters

checks-bios

clipboard

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 4

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

AhnLab-V3	Trojan.Win.Injection.R557217	Alibaba
ALYac	Trojan.GenericKD.65391021	Antiy-AVL
Avast	Trojan.GenericKD.65391021	Avast


```
jedi@eadu:/data/superbowl$ cat superbowl.MACBtime.txt superbowl.body | grep /combase.exe
Tue Feb 07 2023 19:11:06 804352 m... -rwxr-xr-x 0 0 235858 /mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 20:11:38 804352 ...b -rwxr-xr-x 0 0 235858 /mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 20:13:03 804352 ..c. -rwxr-xr-x 0 0 235858 /mnt/windows01/Windows/Temp/combase.exe
Tue Feb 07 2023 20:13:19 804352 .a.. -rwxr-xr-x 0 0 235858 /mnt/windows01/Windows/Temp/combase.exe
aeca0aa59566b054ca9283cfc33e45a4|/mnt/windows01/Windows/Temp/combase.exe|235858|-rwxr-xr-x|0|0|804352|1675797199.806824000|1675793466.0|1675797183.243482800|1675797098.939306100
```

17b6e0bb426b762e1caee67606532e3350d8c752c0625994424916e0fba527ab



55 security vendors and 3 sandboxes flagged this file as malicious

17b6e0bb426b762e1caee67606532e3350

wFCW.exe

peexe assembly runtime-modules detect-

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

Join the VT Community and enjoy additional community insights and c

Security vendors' analysis

AhnLab-V3 Trojan/Win.Injection.R5572

ALYac Trojan.GenericKD.6539102

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 17b6e0bb426b762e1caee67606532e3350d8c752c0625994424916e0fba527ab**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry



Vendor detections: 15

Intelligence 15

IOCs

YARA 2

File information

Comments

Actions

SHA256 hash:

17b6e0bb426b762e1caee67606532e3350d8c752c0625994424916e0fba527ab

SHA3-384 hash:

ad227875abb4faf65fe24d865a7aac69215212abe10461edd1ff7a48bd6c34dc0aa8cf45fa916338e3e7b3b6345f83c

combase.exe | AgentTesla
aka: AgenTesla, AgentTesla, Negasteal
Actor(s): SWEED



Analysis

Category	Package	Started	Completed	Duration	Log	MalScore
FILE	exe	2023-02-23 11:13:55	2023-02-23 11:18:01	246 seconds	Show Log	5.9

Machine

Name	Label	Manager	Started On	Shutdown On	Route
cuckoo1	cuckoo1	VirtualBox	2023-02-23 11:13:56	2023-02-23 11:18:01	inetsim

☰ Mitre ATT&CK	
Command and Control	Execution
<ul style="list-style-type: none">T1071 - Application Layer Protocol<ul style="list-style-type: none">procmem_yara	<ul style="list-style-type: none">T1106 - Native API<ul style="list-style-type: none">antidebug_guardpages

Signatures

- SetUnhandledExceptionFilter detected (possible anti-debug)
- At least one process apparently crashed during execution
- Guard pages use detected - possible anti-debugging.
- Dynamic (imported) function loading detected
- Reads data out of its own binary image
- Creates RWX memory
- Yara rule detections observed from a process memory dump/dropped files/CAPE

Quick Overview

Behavioral Analysis

Network Analysis

Dropped Files (1)

Process Dumps (2)

Payloads (7)

Comments

Compare this analysis to...

Admin

Analysis

Category	Package	Started	Completed	Duration	Log	MalScore
FILE	exe	2023-02-16 08:31:49	2023-02-16 08:36:27	278 seconds	Show Log	7.2

Machine

Name	Label	Manager	Started On	Shutdown On	Route
------	-------	---------	------------	-------------	-------

Signatures

SetUnhandledExceptionFilter detected (possible anti-debug)

A file with an unusual extension was attempted to be loaded as a DLL.

Possible date expiration check, exits too soon after checking local time

Guard pages use detected - possible anti-debugging.

Dynamic (imported) function loading detected

Creates RWX memory

Uses Windows utilities for basic functionality

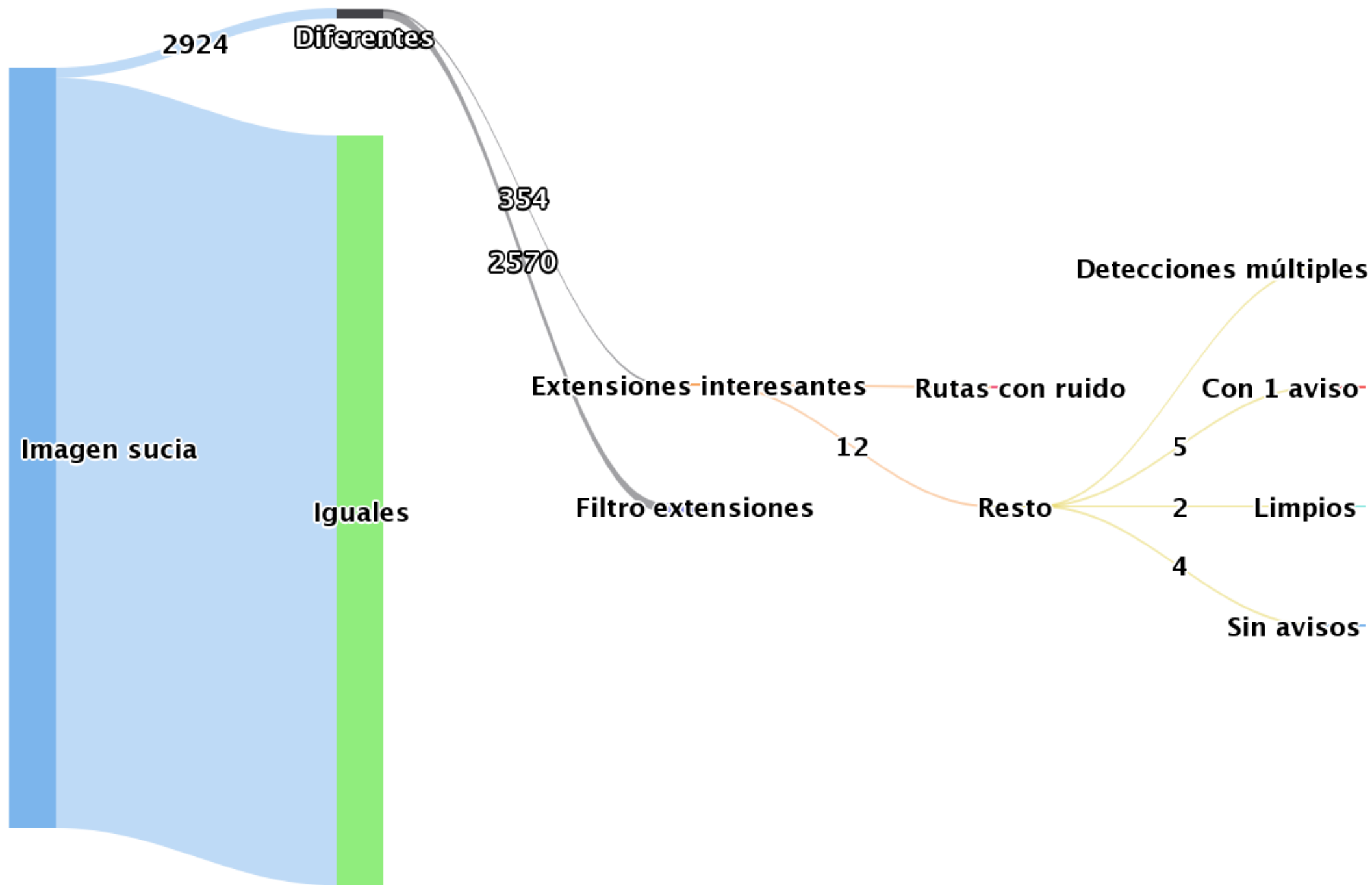
Deletes executed files from disk

Uses suspicious command line tools or Windows utilities

Security vendors' analysis ⓘ

Do you want to automate checks?

Ad-Aware	ⓘ Application.Hacktool.KMSActivator.GH	ALYac	ⓘ Application.Hacktool.KMSActivator.GH
BitDefender	ⓘ Application.Hacktool.KMSActivator.GH	BitDefenderTheta	ⓘ Gen:NN.ZemsilF.34666.tq0@ayVnwRi
CrowdStrike Falcon	ⓘ Win/grayware_confidence_90% (W)	Cybereason	ⓘ Malicious.519abc
Cylance	ⓘ Unsafe	Emsisoft	ⓘ Application.Hacktool.KMSActivator.GH (B)
eScan	ⓘ Application.Hacktool.KMSActivator.GH	ESET-NOD32	ⓘ A Variant Of MSIL /HackKMS I Potentiall



```
bidaidea@h-c0n2023:~$ sudo deluser rafa  
bidaidea@h-c0n2023:~$ sudo deluser luise  
bidaidea@h-c0n2023:~$ cd /  
bidaidea@h-c0n2023:/$ sudo rm -rf *
```



<https://github.com/bidaidea-cyber>
<https://github.com/kero99/macrobber-ng>