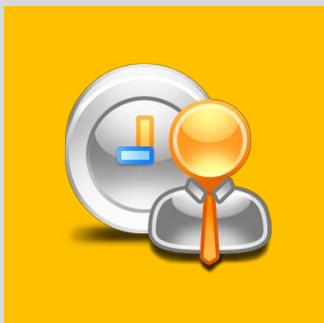
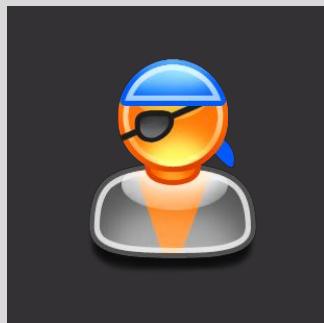


Sony Pictures Hacked, Sent Back To Stone Age

- A Case Study

<http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/>



H

A

c

K

It's a sad thanksgiving to **Sony pictures** as it suffered a massive **data breach**, during the week of Thanksgiving.

The devastating attack was performed by GOP
(Guardians of Peace), an unknown hacker
group.



**YOU HAVE BEEN
HACKED!**

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your Internal data Including your secrets and top secret
If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the 24th, 11:00 PM(GMT).

Data Link :

<https://www.sonypicturesstockfootage.com/SPEData.zip>

<http://dmiplaewh36.spe.sony.com/SPEData.zip>

<http://www.ntcnt.ru/SPEData.zip>

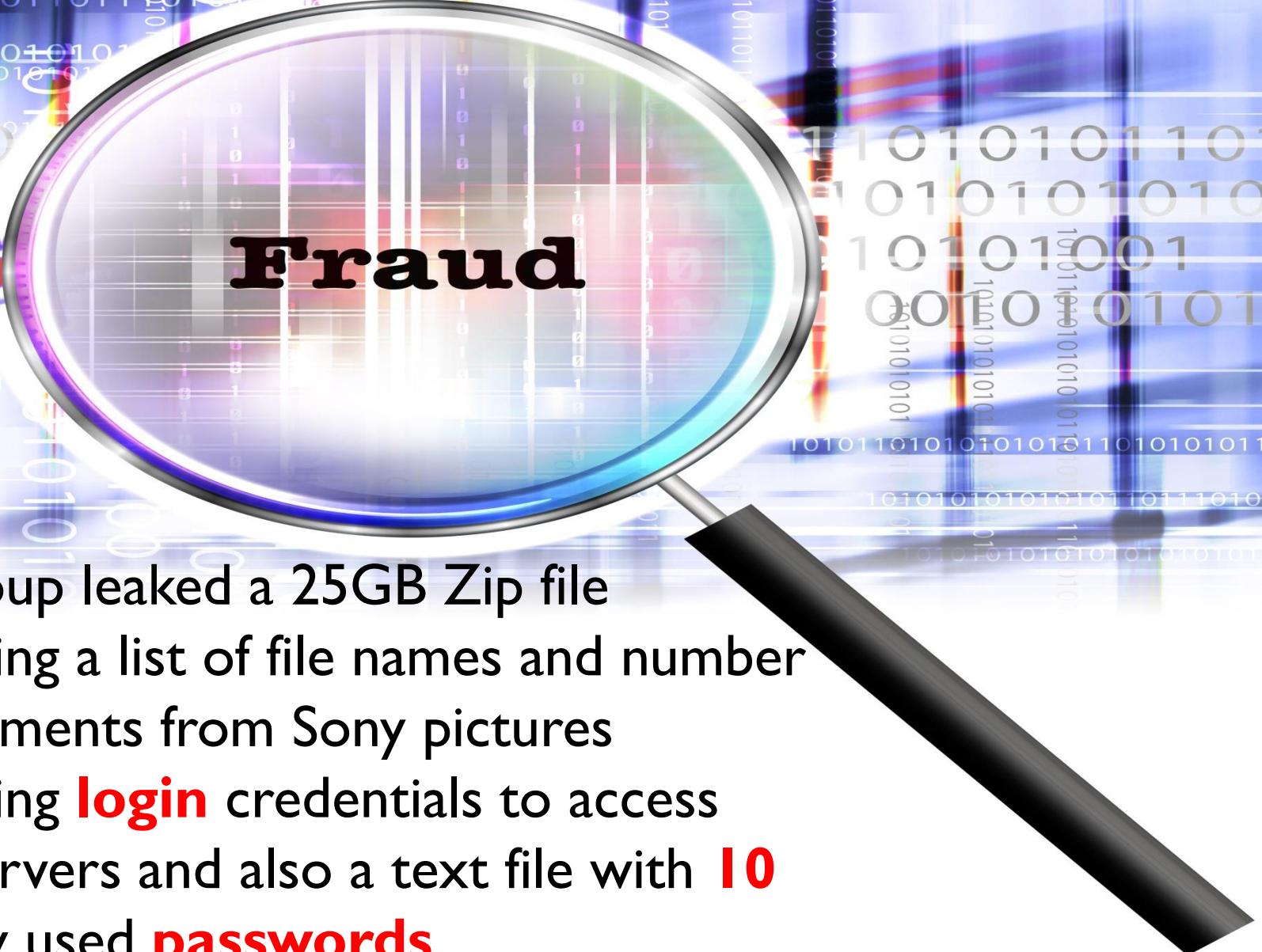
<http://www.thammasatpress.com/SPEData.zip>

<http://moodle.universidadebematech.com.br/SPEData.zip>

The above picture was displayed on the **victim's** system during the hack warning about unspecified **demands** and the links of **data files**.

The devastating hack included leaking of **5** full length **movies** which are yet to be released and nearly 47000 **social security** numbers including **personal** data such as employee salary information, home address and list of freelancers in unprotected excel sheets. The salary documents reveal **gender pay** discrepancy in Sony.



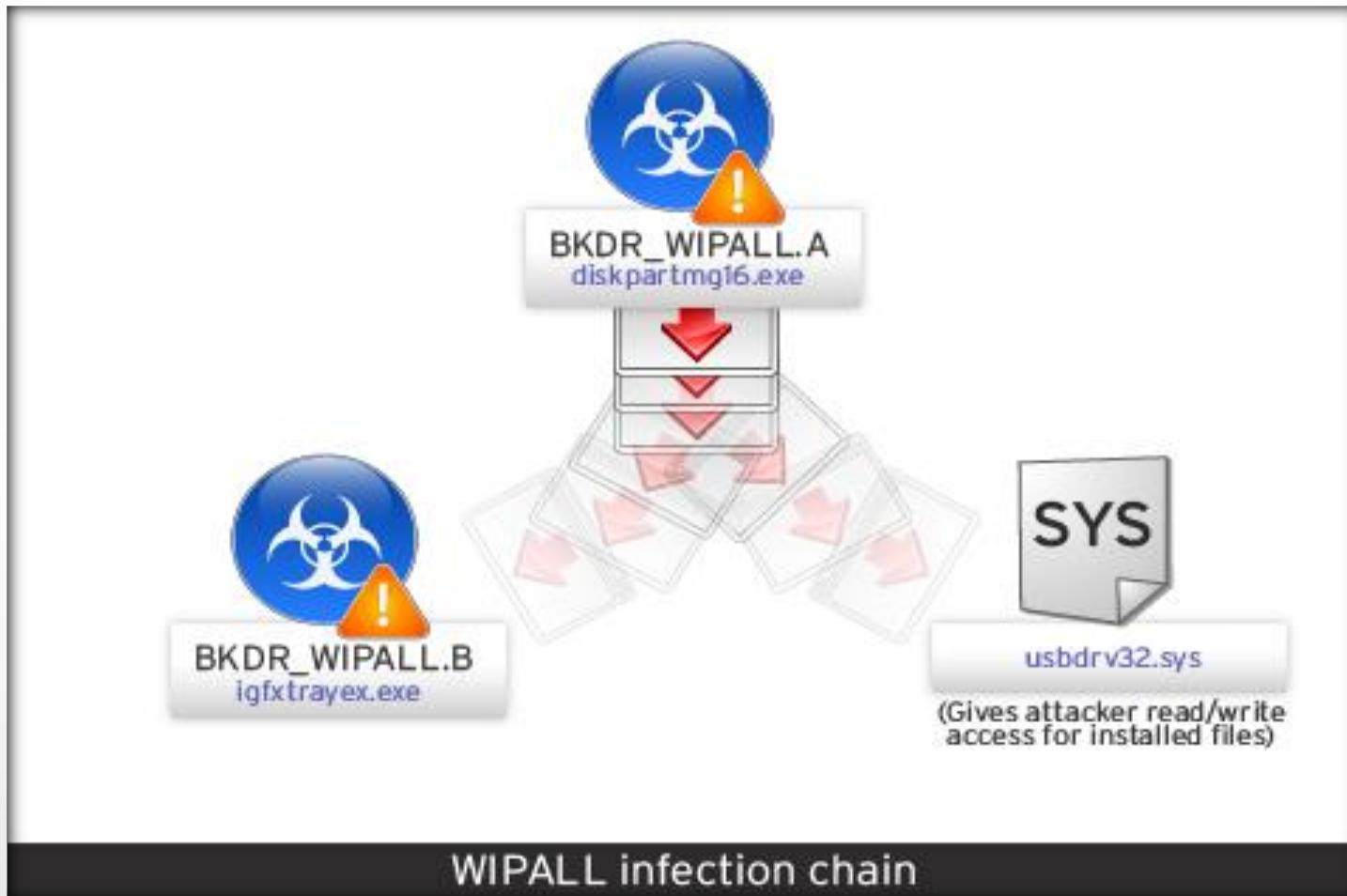


Fraud

The group leaked a 25GB Zip file containing a list of file names and number of documents from Sony pictures containing **login** credentials to access their servers and also a text file with **10** recently used **passwords**.



The dropper, **Troj/Destover-C** installs itself as a windows service.



It creates a Windows file sharing using “%SystemRoot%” Windows environmental variable which points to the Windows Directory containing the system files and gives **unrestricted** access to the directory.

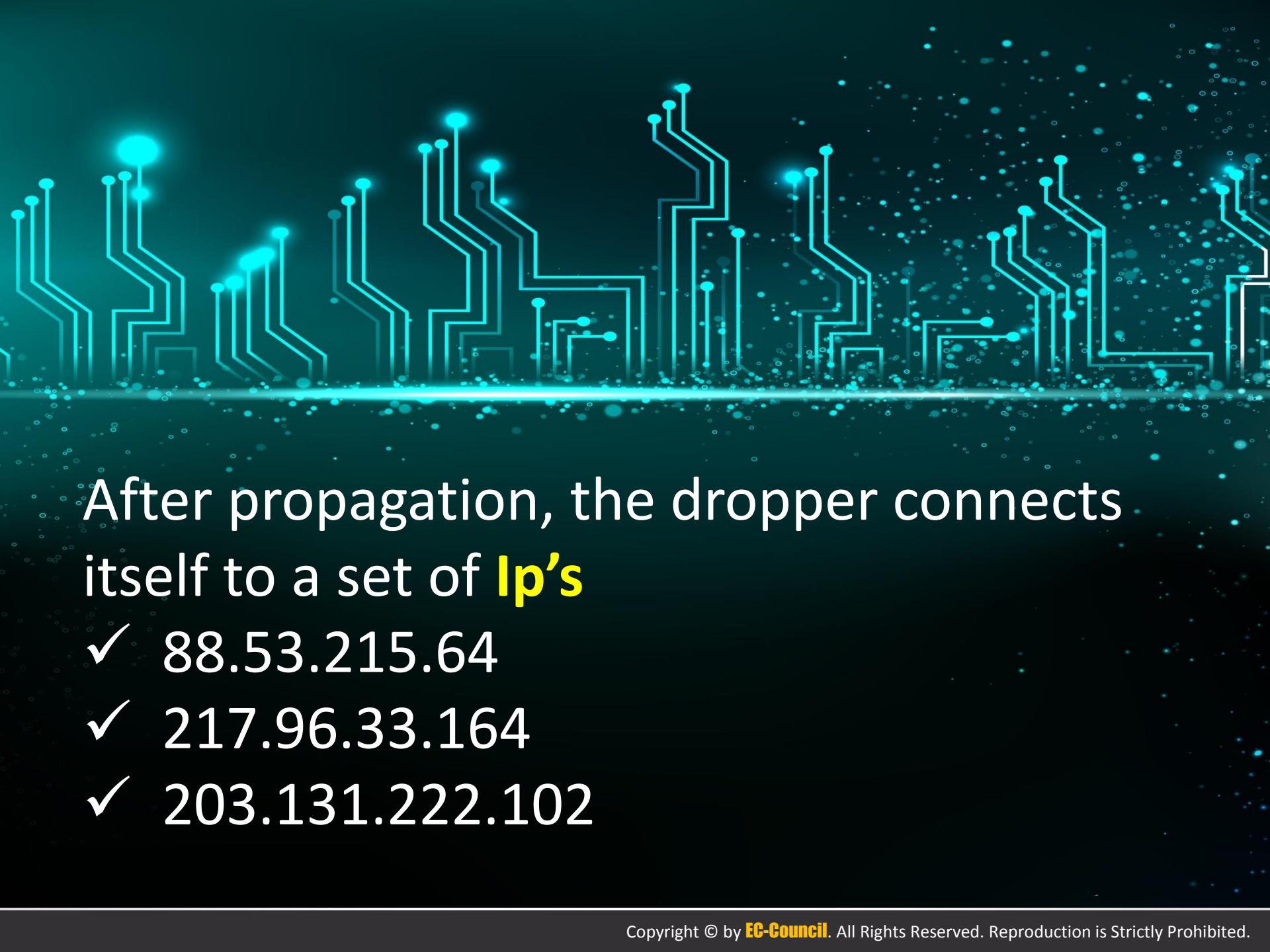


Then it uses the command line of **WMI** to launch the code on other systems to propagate.



The **malicious** files propagated are:

- ✓ diskpartmg16.exe
- ✓ net_ver.dat
- ✓ **igfxtrayex.exe**
- ✓ iissvr.exe



After propagation, the dropper connects itself to a set of **Ip's**

- ✓ 88.53.215.64
- ✓ 217.96.33.164
- ✓ 203.131.222.102

Hard **Code** with **Ip's** Embedded into it.

```
rule unknown_wiper_error_strings{  
    meta: unique custom error debug strings discovered in the wiper malware  
    strings:  
        $IP1 = "203.131.222.102" fullword nocase  
        $IP2 = "217.96.33.164" fullword nocase  
        $IP3 = "88.53.215.64" fullword nocase  
        $MZ = "MZ"  
    condition:  
        $MZ at 0 and all of them  
}
```

The dropper also installs the file **iissrv.exe** same as in IIS and listens on port **80**. The file which is an internal web server is used to display the **scrolling text** and **JPEG** images on the victim's system at **Sony**.



Now, a windows exe file '**igfxtrayex.exe**' starts to work. It drops **several** copies of itself and starts executing using **four** different commands.

- ✓ -i (Backup)
- ✓ -m (mbr overwrite)
- ✓ -d (data overwrite)
- ✓ -w (web server)

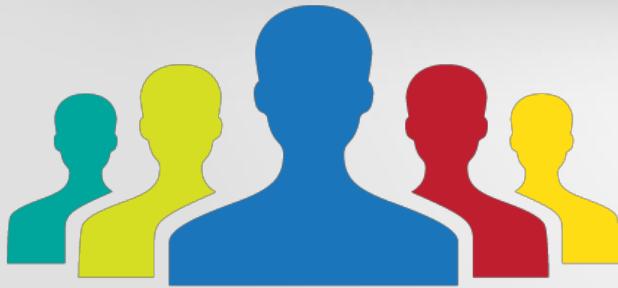
-m command tries to connect to Ip addresses and gets the compressed **EldoS RawDisk** driver, and writes it out to the temp directory as a '**usbdrv3.sys**' and starts usbdrv3 service '**USB 3.0 Host Controller**'.





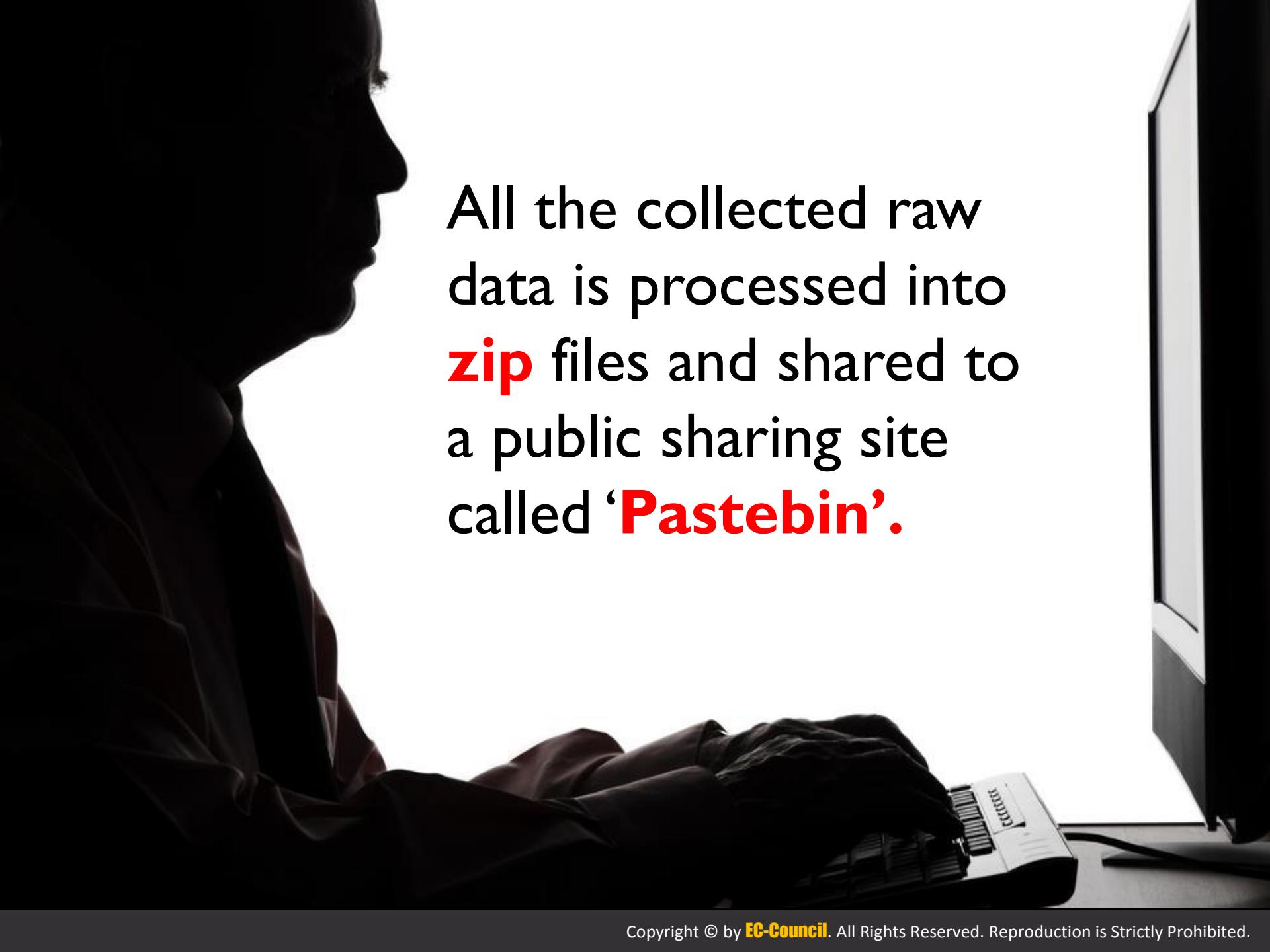
It starts the driver service and closes its service handle.
It then creates a **filehandle** to the driver with write permissions and writes to that handle with **64k strings** of '**0xAAAAAAAAAA**'. ← It then creates new threads, each of which attempts to connect to any **physical drive** letter and overwrite them as well.

The **-d (data overwrite)** command executes and attempts to connect to the **Ips** again. It traverses through all data files (**exe and dll**) and overwrites file contents with '**0x0df0adba**' in a 20k chunk in **user mode** without the need to administrative privileges and it attempts to delete the data file using the win32 api 'DeleteFileW' and attempts to delete .exe and .dll files.



-w (web server) tries to connect to the Ip again and uses '**cmd.exe /c net stop termservice /y**' command to stop the Windows terminal services and finds resource#85, decompresses and writes contents out to '**'c:\windows\iissvr.exe'**' launching the iissvr.exe process and exits.



A dark silhouette of a person's head and shoulders, facing right, is positioned on the left side of the frame. Their hands are visible at the bottom, resting on a keyboard. To the right, a portion of a computer monitor is visible.

All the collected raw
data is processed into
zip files and shared to
a public sharing site
called '**Pastebin**'.

Pastebin Showing the Links to Shared files:

The screenshot shows the Pastebin homepage with a navigation bar at the top. Below the bar, a specific paste titled "Sony Breach Torrents" is displayed. The paste content lists various URLs and instructions related to a Sony breach. A VULTR advertisement is overlaid on the page.

PASTE BIN | #1 paste tool since 2002

create new paste | trending pastes

Follow @pastebin | Like - 193k

search...

sign up | login | my alerts

Want more features on Pastebin? Get a premium account!

Sony Breach Torrents

BY: A GUEST ON DEC 4TH, 2014 | SYNTAX: NONE | SIZE: 2.81 KB | VIEWS: 676 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

LARGEST CLOUD SERVER NETWORK

VULTR

Spin up VPS on 6 continents!

1. You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses.
2. These are all confidential and include data related to sales plan of SPE.
3.
4. Password: diespe123
5.
6. 1. List of computers in Sony Pictures hacked by GOP
7. <http://ge.tt/15YQ9z52/v/0>
8. <http://rghost.net/59405536>
9. <http://180upload.com/gpu5oqh4iqri>
10.
11. 2. Special bonus to the friends of GOP
12. <http://ge.tt/7w2Lny52/v/0>
13. <http://rghost.net/59402539>
14. <http://180upload.com/yw5hcvvmt0nr>
15.

**To know more about these
attacks and how to secure your Information
Systems become a Certified Ethical Hacker**