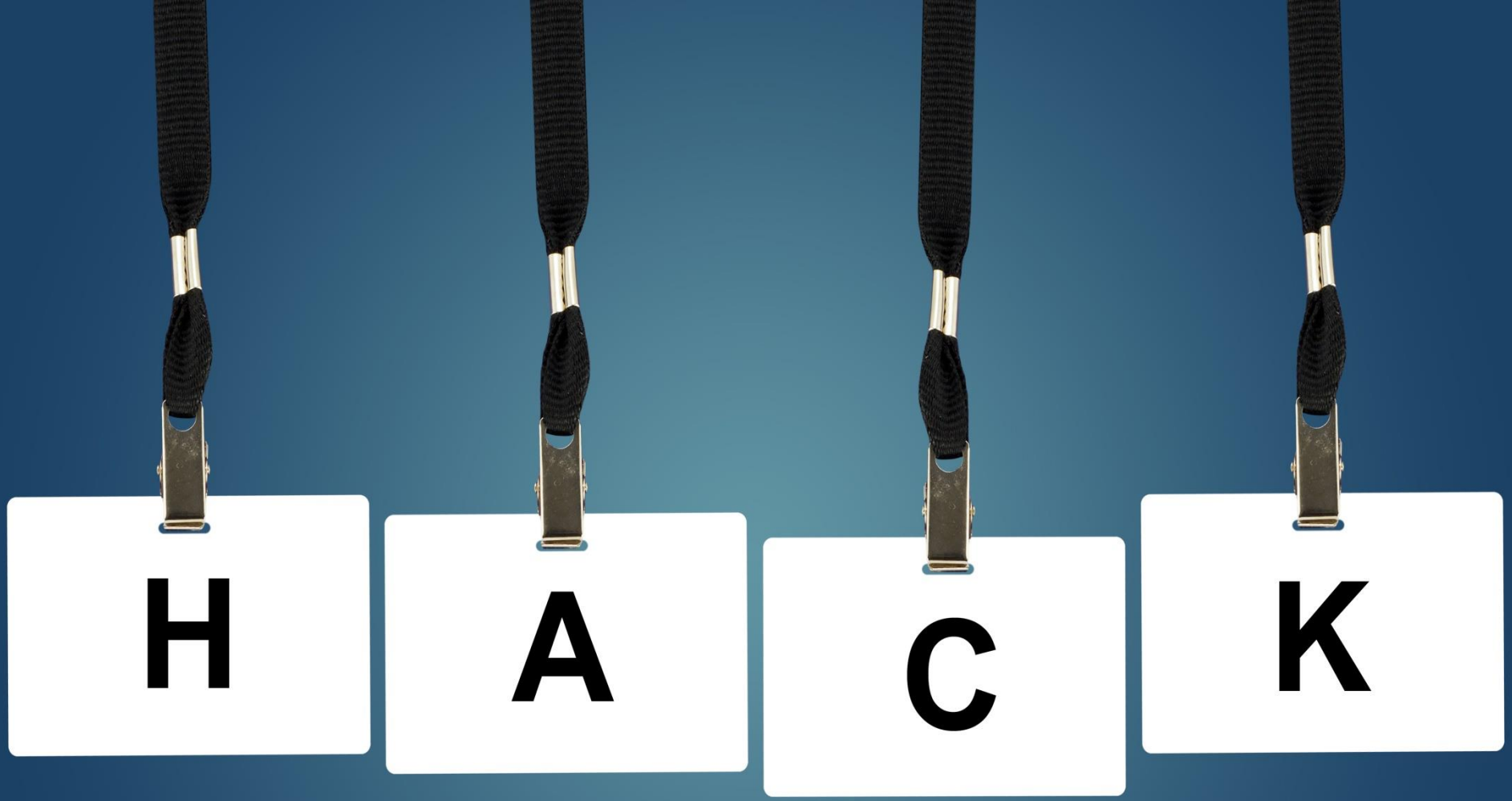
Sony Pictures Hacked, Sent Back To Stone Age

- A Case Study

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





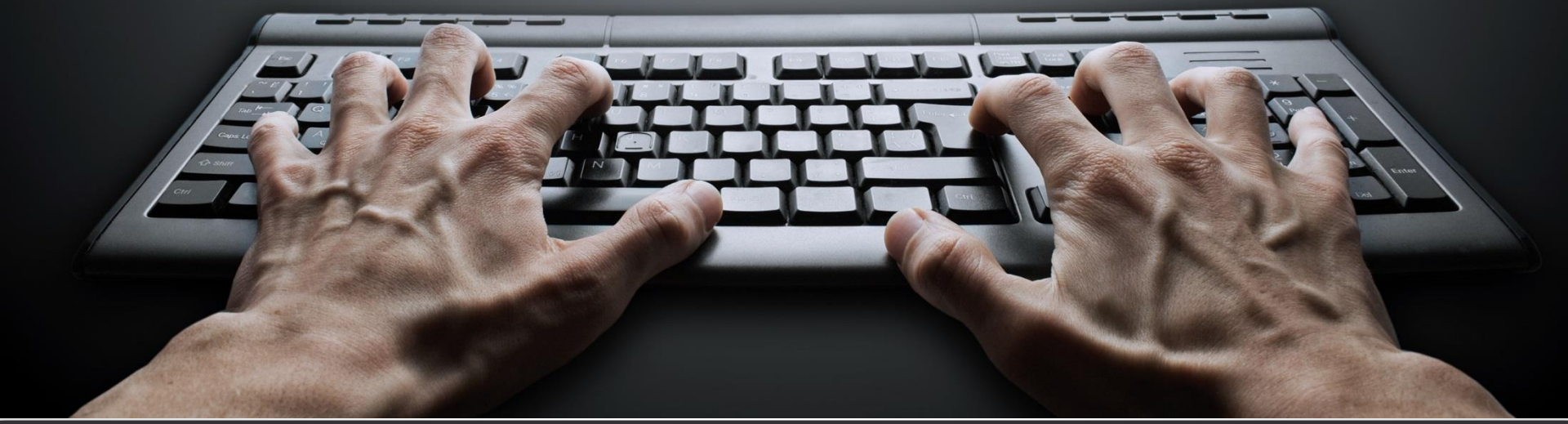


It's a sad thanksgiving to **Sony pictures** as it suffered a massive **data breach**, during the week of Thanksgiving.

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

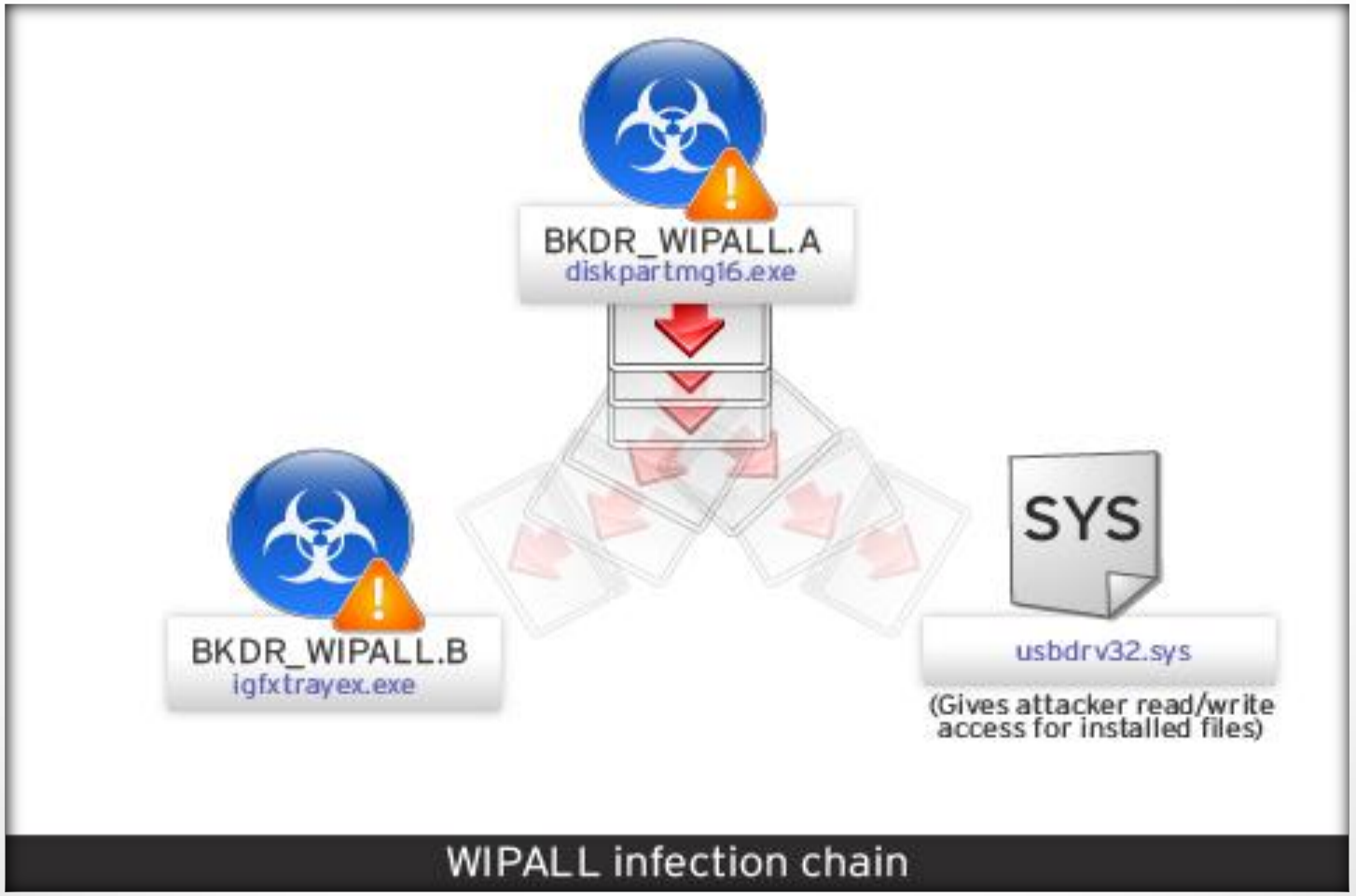
The above picture was displayed on the **victim's** system during the hack warning about unspecified **demands** and the links of **data files.**

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.



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.



WIPALL infection chain

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.

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**.

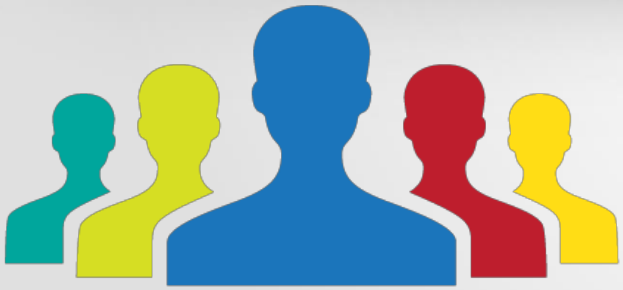
Now, a windows exe file **'igfxtrayex.exe'** starts to work. It drops **several** copies of itself and starts executing using **four** different commands.

- ✓ -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'.

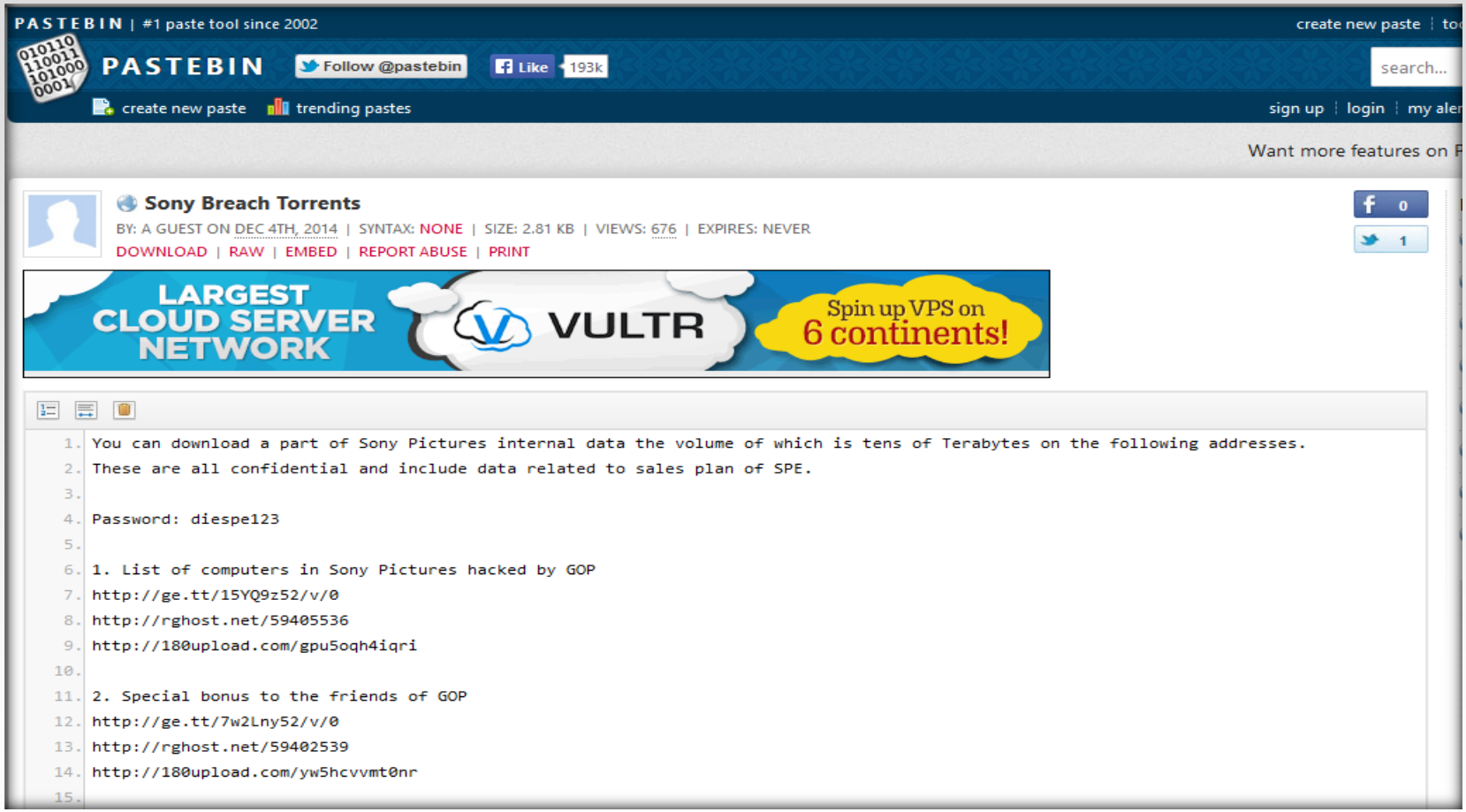
It starts the driver service and closes its service handle.
It then creates a **filehandle** to the driver with write permissions and writes to that handle with **64k strings** of '**0xAAAAAAAA**'. ← It then creates new threads, each of which attempts to connect to any **physical drive** letter and overwrite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

Pastebin Showing the Links to Shared files:



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