Printer Security

INSIGHT INTO THE PRINTERS

$: whoami

Nishant Grover

Interest: Incident Response, Scripting, threat hunting

@ngrovyer

$: Why printers?

$: Why printers?

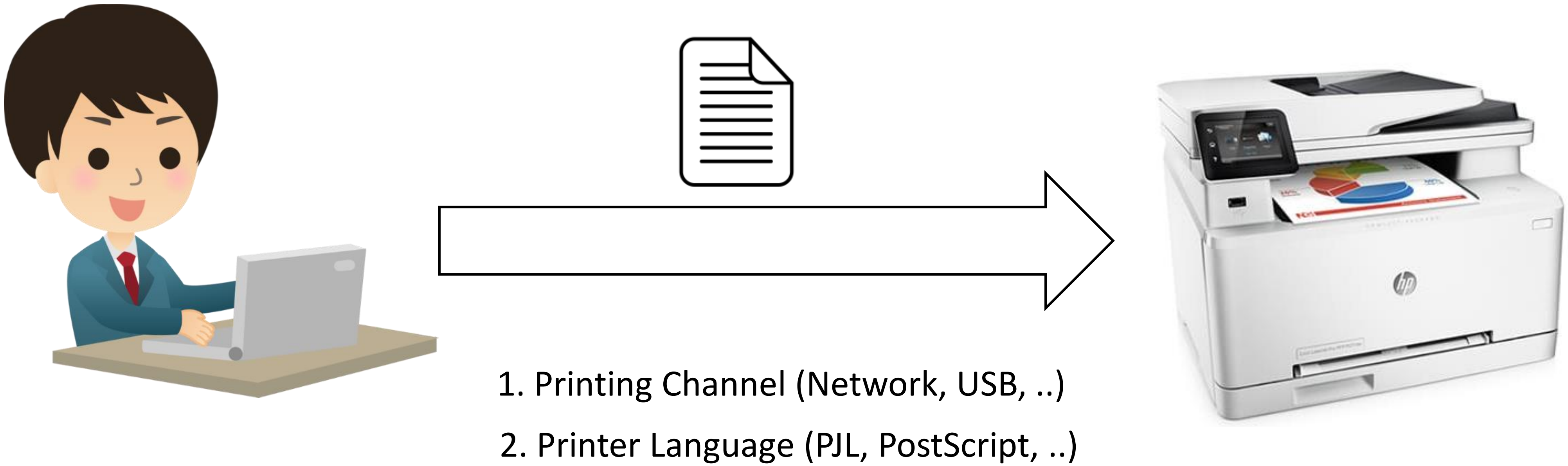
- A company has multiple offices, multiple printers!
- Any business, any house hold will have them
- Printers are in our networks!
- They have sensitive information, like business contract, patient records, etc
- They might be weakest link in your IT Networks!

$: Printers Evolution

$: Problems in Current Printers?

- Access Printer file system, through Print Job
- Access Printer Memory, through Print Job
- Firmware Update, you guessed it right.
- Printers are problematic by design, they don’t segregate Print Jobs and Administrative tasks
- Everything goes from same channel
- Default Passwords, Information Disclosure, etc, etc

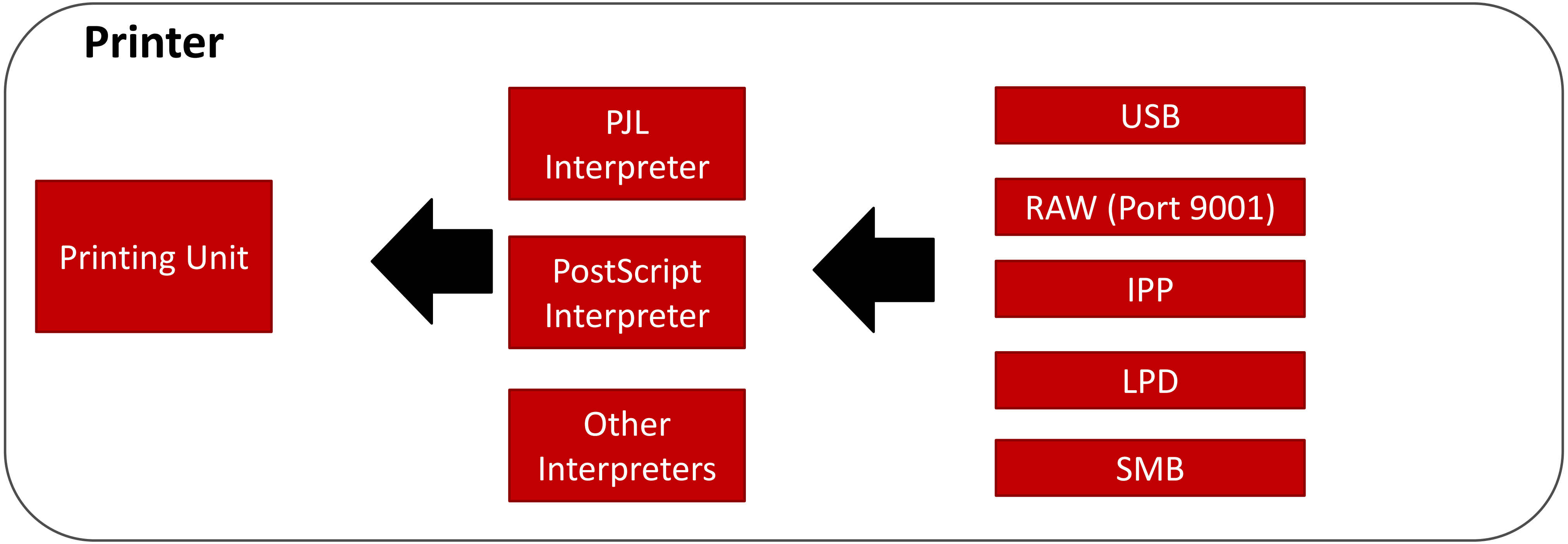
$: How to Print



1. Printing Channel (Network, USB, ..)

2. Printer Language (PJL, PostScript, ..)

$: Printer Internals



$: PJL

- Developed by HP, defacto for print Jobs
  - @PJL SET PAPER=A4
  - @PJL SET COPIES=10

- Not limited to current Print Job, Potential to influence other print jobs

$: PostScript

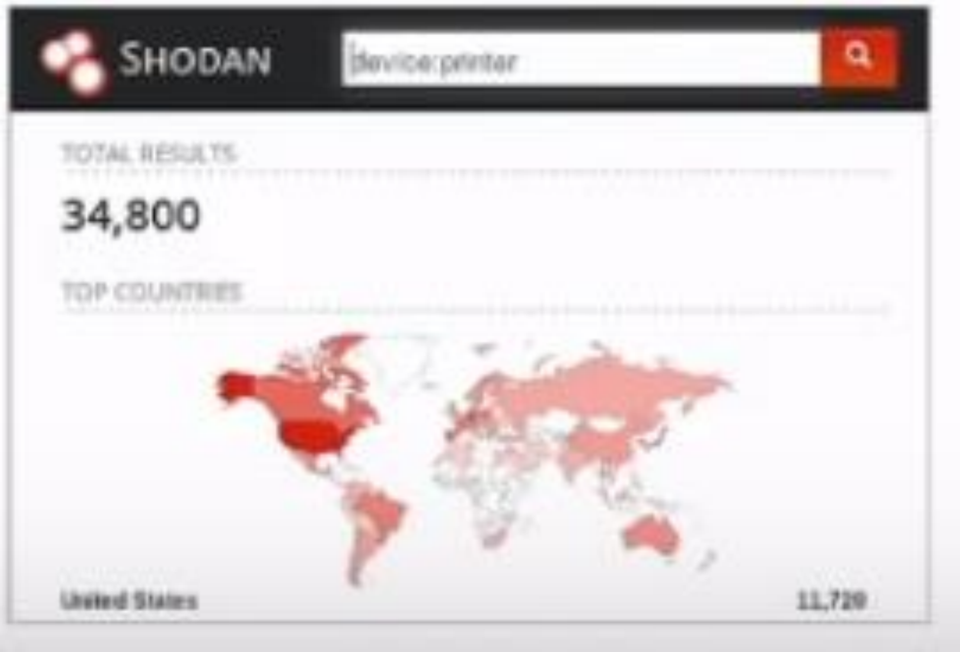
- Developed by Adobe (1982-1984)
- Heavily used on Laser Printers
- Turing Complete Language i.e. you by default get access to execute any code

$: Attacks

- Print through USB
  - Infect the Printer using PostScript malware, Permanently
- Print through Internet
  - Connect to Port 9001 of printer and get bi-directional connection
- Print on Network
  - Simple Print Job

$: Online Printers

Print through Internet



SHODAN device:printer

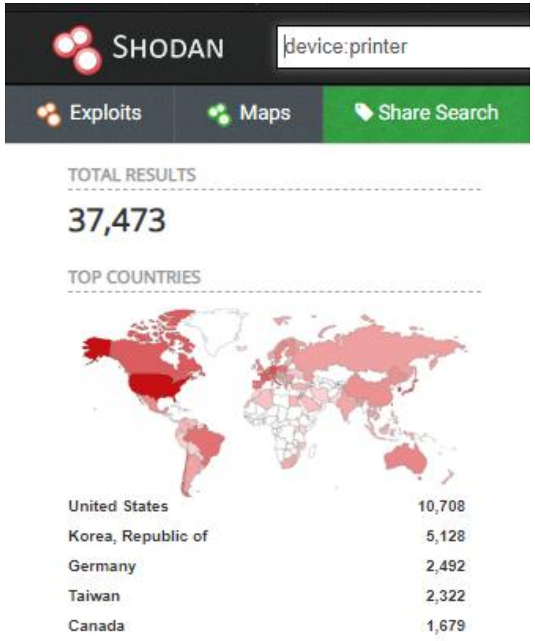
TOTAL RESULTS

34,800

TOP COUNTRIES

United States	11,720

2017



SHODAN device:printer

Exploits · Maps · Share Search

TOTAL RESULTS

37,473

TOP COUNTRIES

United States	10,708
Korea, Republic of	5,128
Germany	2,492
Taiwan	2,322
Canada	1,679

2019

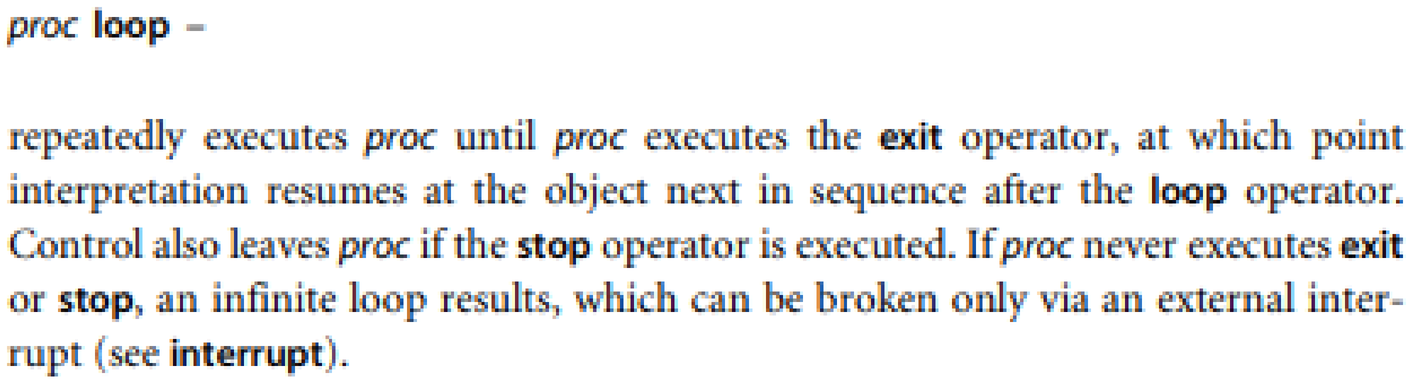
$: Classes of Attacks

- Denial of Service
- Protection Bypass
- Print Job Manipulation
- Information Disclosure

$: Denial of Service

PostScript – Infinite Loop

{} loop



proc **loop** –

repeatedly executes *proc* until *proc* executes the **exit** operator, at which point interpretation resumes at the object next in sequence after the **loop** operator. Control also leaves *proc* if the **stop** operator is executed. If *proc* never executes **exit** or **stop**, an infinite loop results, which can be broken only via an external interrupt (see **interrupt**).

Unless you restart the printer

$: Denial of Service

Physically Damage the device

Uses NVRAM for permanent Settings

Have limited Number of Write cycles (usually in Millions)

NVRAM Settings can be changed via Print Jobs!

Continuously Set long-term values of number of copies

@PJL DEFAULT COPIES=X

$: Denial of Service (PassBack attacks)

Printer Communicates to you

- Log Into the printer
- Look for LDAP Server IP Configured
- Change it to your Machine IP
- Netcat –l –vv –p 444
- Wait for Credentials!

$: Protection Bypass

Bypassing password mechanism

Pressing certain keys on Keyboard (if you have physical access)

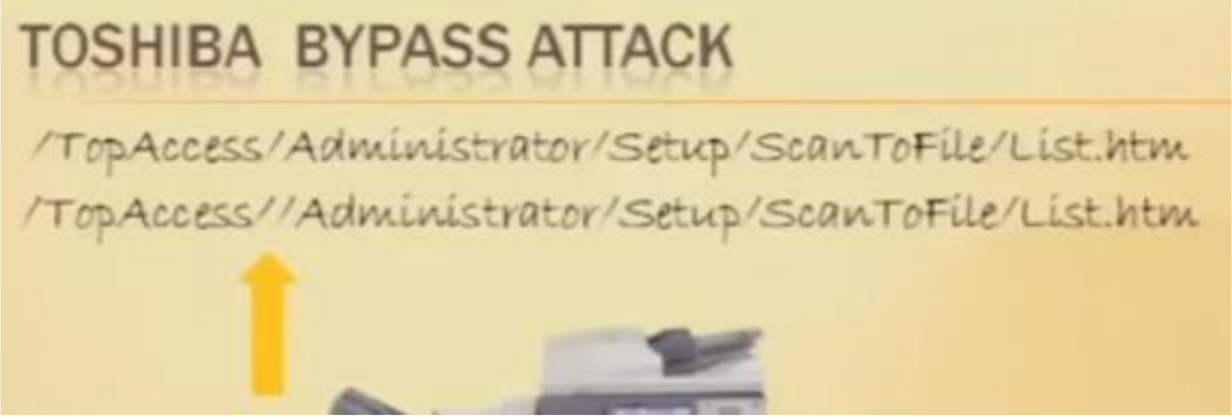
OR PJL String

@PJL DMCD ASCIIHEX= “040006020501010301040106”

RESETS THE HP PRINTER TO FACTORY DEFAULT

$: Protection Bypass

Buggy Web User Interface



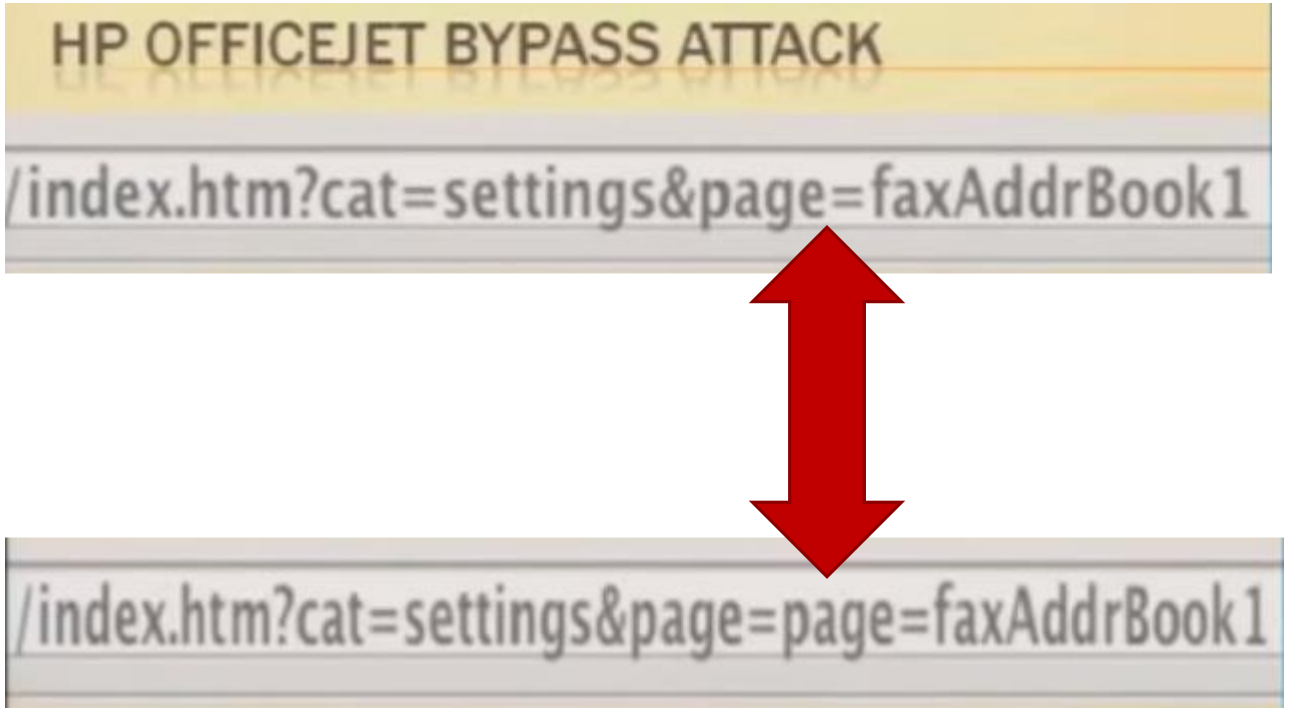
TOSHIBA BYPASS ATTACK

/TopAccess/Administrator/Setup/ScanToFile/List.htm

/TopAccess//Administrator/Setup/ScanToFile/List.htm

$: Protection Bypass

Buggy Web User Interface



HP OFFICEJET BYPASS ATTACK

```
/index.htm?cat=settings&page=faxAddrBook1
```

```
/index.htm?cat=settings&page=page=faxAddrBook1
```

$: Protection Bypass

Leveraging Default Password

Username: Admin
Password: 123456

http://www.phenoelit.org/dpl/dpl.html

$: Print Job Manipulation

Redefinition of PostScript showpage operator

Its contained in every page, every document it prints

Need to provide an .eps file

Replace certain strings in user files

Introduce Typos & mistakes

Change numbers in finance related document

$: Information Disclosure

- Capture Print Jobs
  - Save on file system or memory

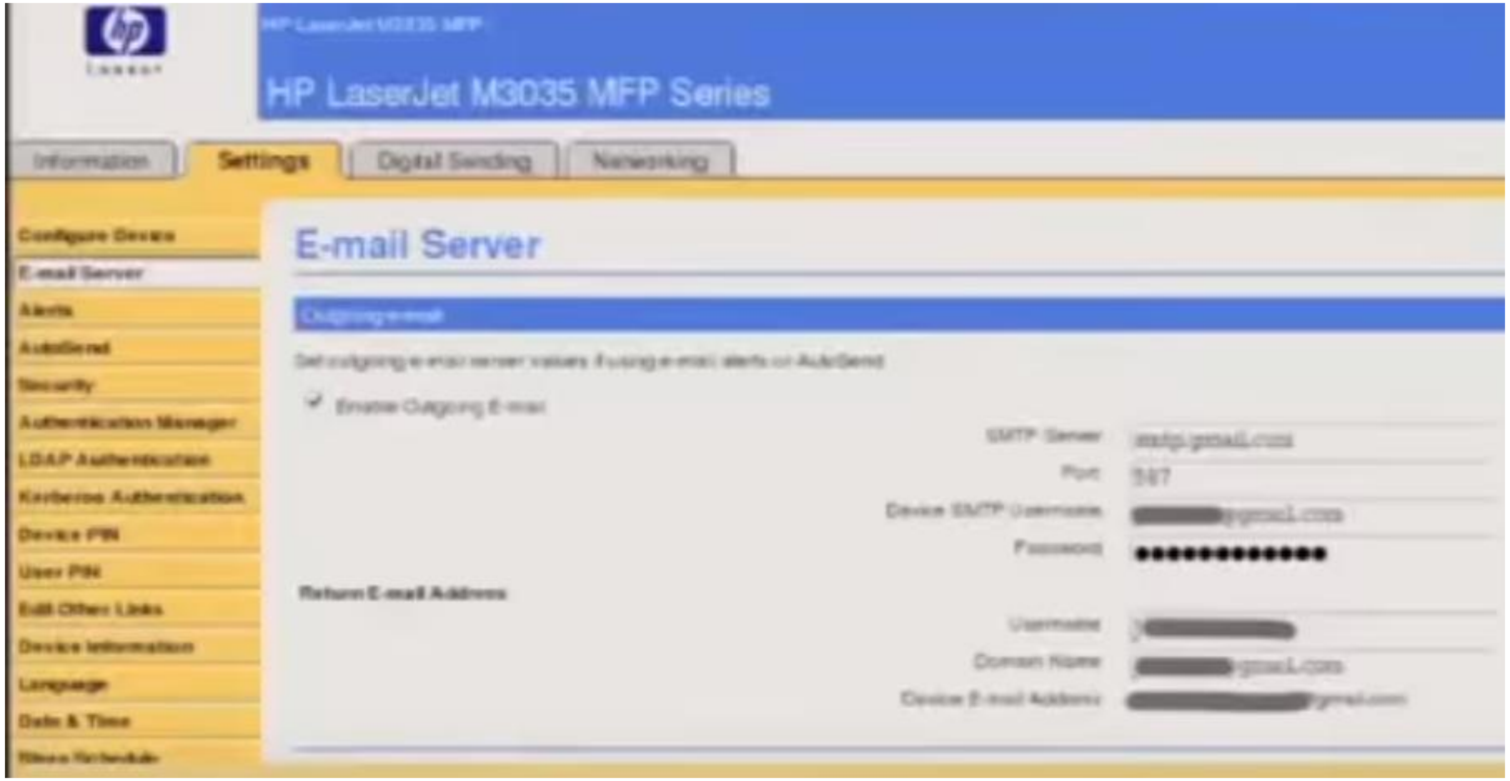
- Unprotected Direct URL Pages
- Pulling out Backup configs

$: Information Disclosure

- Access to Memory
- Access to Printer file system
  - IPSec Preshared Keys
  - LDAP Passwords
  - Email Passwords
  - FTP Credentials
  - Wifi Passwords

$: Information Disclosure

Email Passwords



HP LaserJet M3035 MFP

HP LaserJet M3035 MFP Series

E-mail Server

Outgoing e-mail

Set outgoing e-mail server values if using e-mail alerts or AutoSend

☑ Enable Outgoing E-mail

SMTP Server: smtp.gmail.com

Port: 587

Device SMTP Username: [redacted]@gmail.com

Password: ●●●●●●●●●●●●●

Return E-mail Address

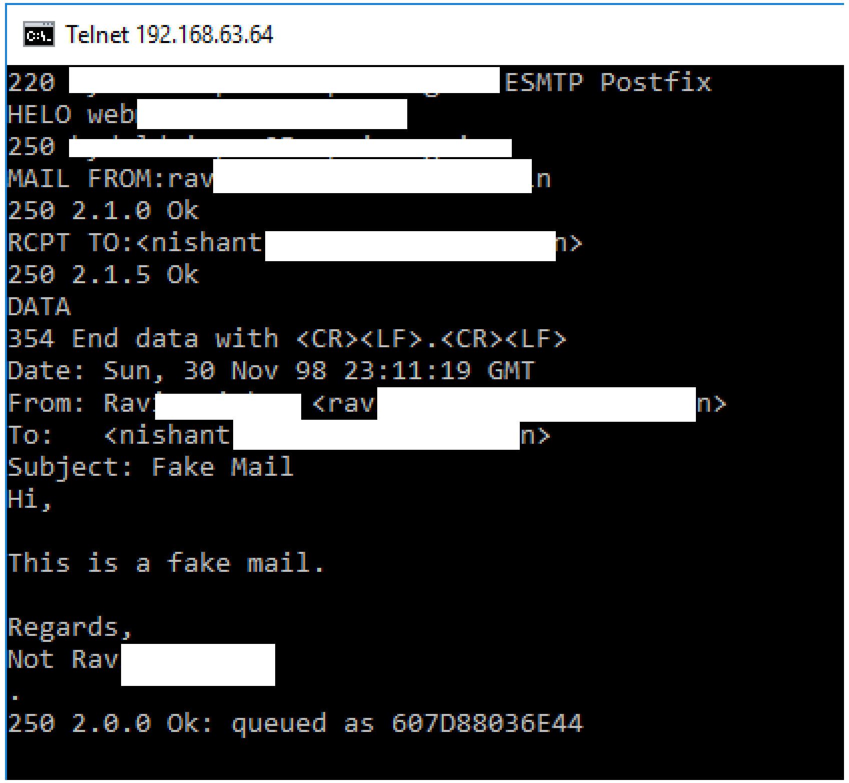
Username: [redacted]

Domain Name: [redacted]gmail.com

Device E-mail Address: [redacted]@gmail.com

$: Information Disclosure

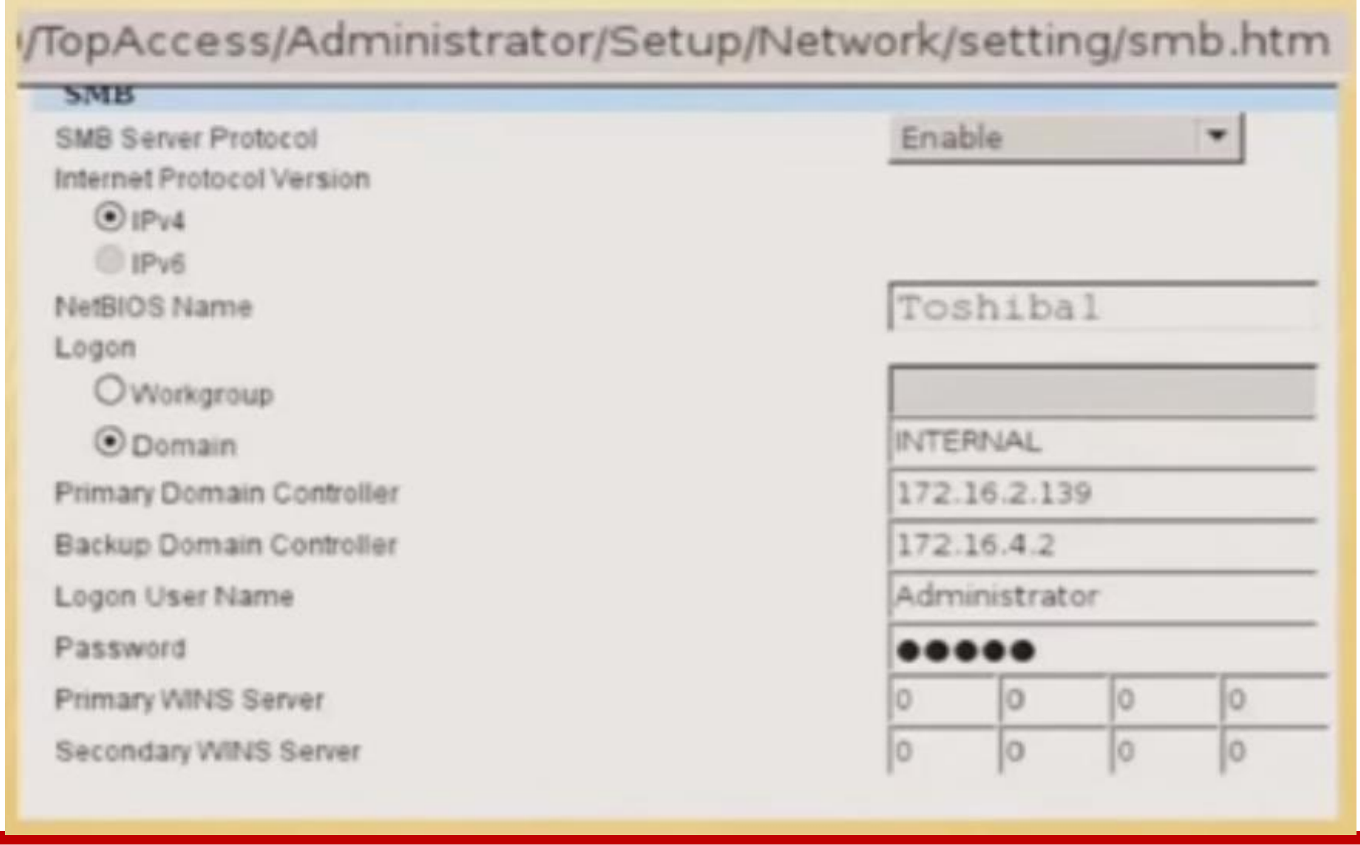
Email Passwords



```
220 [redacted] ESMTP Postfix
HELO web[redacted]
250 [redacted]
MAIL FROM:rav[redacted]n
250 2.1.0 Ok
RCPT TO:<nishant[redacted]n>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Sun, 30 Nov 98 23:11:19 GMT
From: Rav[redacted] <rav[redacted]n>
To:   <nishant[redacted]n>
Subject: Fake Mail
Hi,

This is a fake mail.

Regards,
Not Rav[redacted]
.
250 2.0.0 Ok: queued as 607D88036E44
```

$: Information Disclosure

LDAP Passwords



/TopAccess/Administrator/Setup/Network/setting/smb.htm

SMB

SMB Server Protocol	Enable
Internet Protocol Version	
◉ IPv4	
○ IPv6	
NetBIOS Name	Toshiba1
Logon	
○ Workgroup	
◉ Domain	INTERNAL
Primary Domain Controller	172.16.2.139
Backup Domain Controller	172.16.4.2
Logon User Name	Administrator
Password	●●●●●
Primary WINS Server	0 0 0 0
Secondary WINS Server	0 0 0 0

$: PS to PDF Websites

Send Malicious .PS files to Converter Websites

Get Underlying Information of there systems

Also extend to Image files, .EPS files which contains PostScript commands

$: Printing from the Web

A script that scanned for insecure public-facing devices with open

RAW – 9100 Port

Internet Printing Protocol – 631 Port

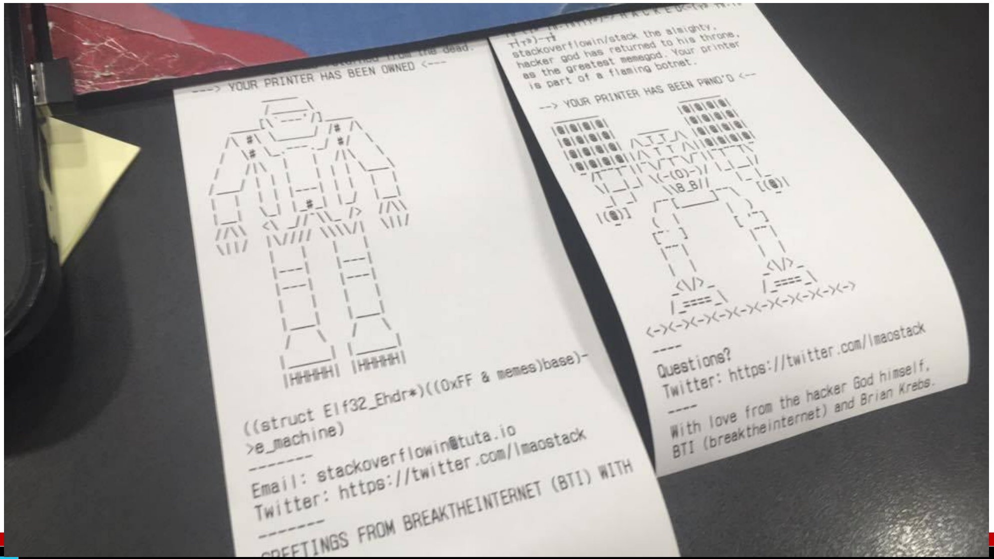
Line Printer Remote services – 515 Port

$: Countermeasures

Don’t connect your printer online – directly to internet

Hacker: I made 160,000 printers spew out ASCII art around the world

Check your firewalls, people – no need to leave all this gear facing the internet



```
---> YOUR PRINTER HAS BEEN OWNED <---

((struct Elf32_Ehdr*)((0xFF & memes)base)-
>e_machine)
--------
Email: stackoverflowin@tuta.io
Twitter: https://twitter.com/lmaostack
--------
GREETINGS FROM BREAKTHEINTERNET (BTI) WITH
```

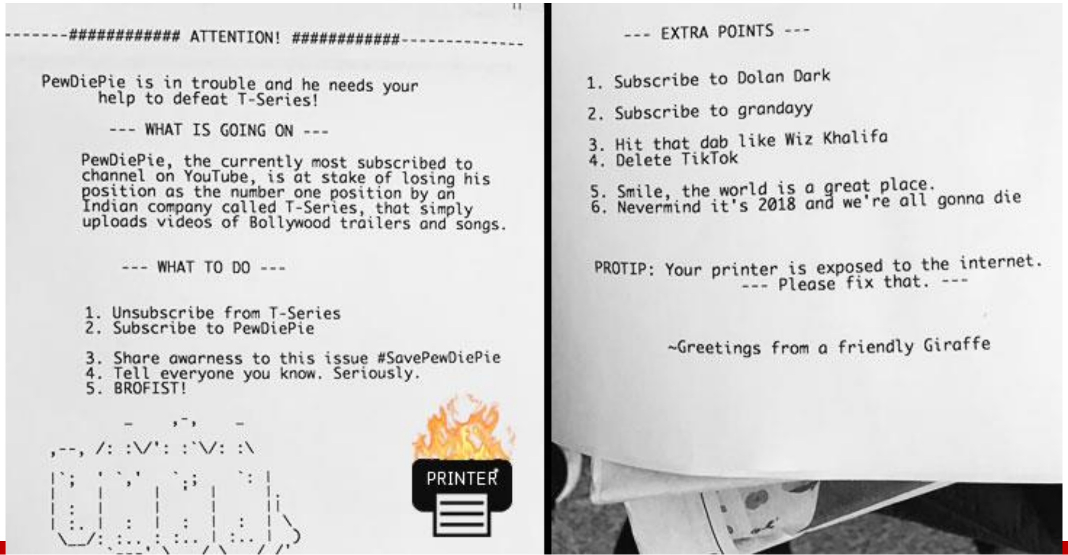
```
stackoverflowin/stack the almighty,
hacker god has returned to his throne,
as the greatest memegod. Your printer
is part of a flaming botnet.

--> YOUR PRINTER HAS BEEN PWND'D <--

----
Questions?
Twitter: https://twitter.com/lmaostack
----
With love from the hacker God himself,
BTI (breaktheinternet) and Brian Krebs.
```

PewDiePie printer hackers strike again

By Joe Tidy
BBC Cyber-security reporter

16 December 2018

Share



```
-------############ ATTENTION! ############-------------

PewDiePie is in trouble and he needs your
    help to defeat T-Series!

    --- WHAT IS GOING ON ---

  PewDiePie, the currently most subscribed to
  channel on YouTube, is at stake of losing his
  position as the number one position by an
  Indian company called T-Series, that simply
  uploads videos of Bollywood trailers and songs.

      --- WHAT TO DO ---

  1. Unsubscribe from T-Series
  2. Subscribe to PewDiePie

  3. Share awarness to this issue #SavePewDiePie
  4. Tell everyone you know. Seriously.
  5. BROFIST!
```

```
    --- EXTRA POINTS ---

1. Subscribe to Dolan Dark

2. Subscribe to grandayy

3. Hit that dab like Wiz Khalifa
4. Delete TikTok

5. Smile, the world is a great place.
6. Nevermind it's 2018 and we're all gonna die


PROTIP: Your printer is exposed to the internet.
          --- Please fix that. ---


      ~Greetings from a friendly Giraffe
```

$: Countermeasures

Make Physical Access of Device difficult

Sandbox printers into separate VLANs and are reachable from Print Servers

Vendors to move over from insecure PJL and PostScript

$: References

S.No	Description	Link
1	Printer Exploitation ToolKit	http://bit.ly/nullmeetfeb1
2	Exploiting Network Printers (BlackHat 2017)	http://bit.ly/nullmeetfeb2
3	Hacking an Office Network through Printer (Defcon 2014)	http://bit.ly/nullmeetfeb3
4	Hacking Printers Wiki	http://bit.ly/nullmeetfeb4
5	Printer Hacking Resources	http://bit.ly/nullmeetfeb5
6	PRAEDA Tool	http://bit.ly/nullmeetfeb6
7	PJL Technical Reference Guide – 176 Pages	http://bit.ly/nullmeetfeb7
8	PJL Technical Reference Manual – 342 Pages	http://bit.ly/nullmeetfeb8
9	PostScript Language Reference Guide – 912 Pages	http://bit.ly/nullmeetfeb9
10	PostScript BlueBook – Tutorial and Cookbook – 242 Pages	http://bit.ly/nullmeetfeb10

>>> sys.exit()

Thanks!

Any questions