Printer Hacking Intro

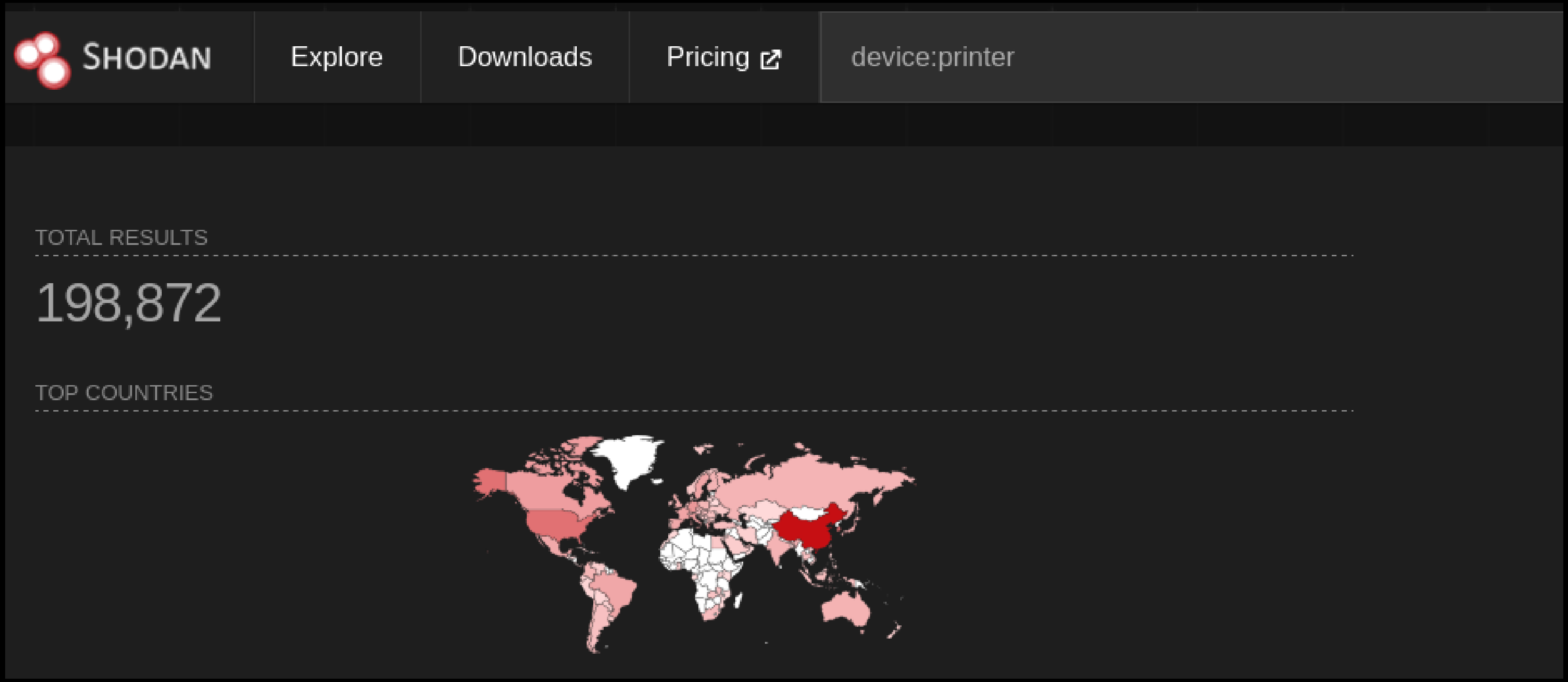
Matěj Smyčka

Whoami

- Vulnerability management at CSIRT-MU
- Studying at FI MU – Software Engineering
- Thesis on writing templates for Nuclei

Motivation

- Sensitive data exfiltration
- Monetary damages/DOS
- Lateral movement
- Botnets
- …

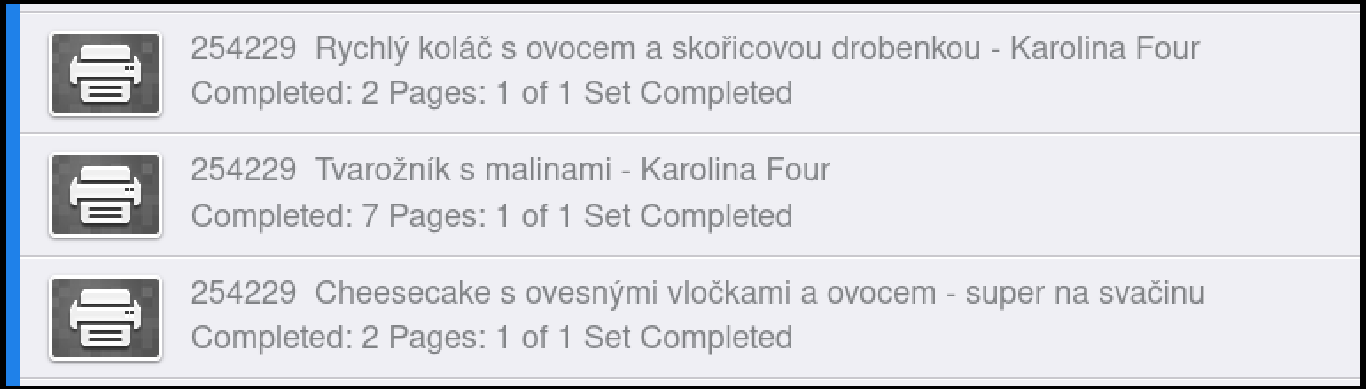


TOTAL RESULTS

198,872

TOP COUNTRIES

HTTP Interface

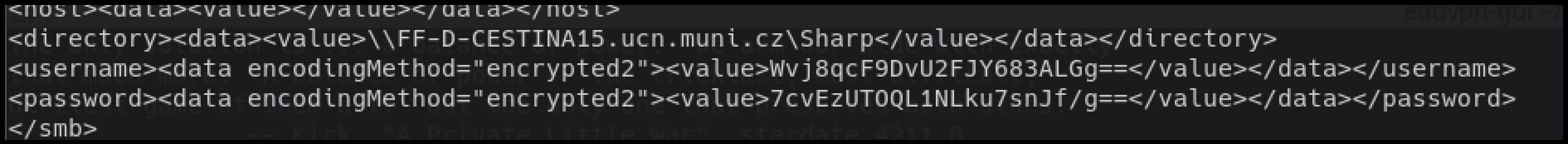


254229 Rychlý koláč s ovocem a skořicovou drobenkou - Karolina Four
Completed: 2 Pages: 1 of 1 Set Completed

254229 Tvarožník s malinami - Karolina Four
Completed: 7 Pages: 1 of 1 Set Completed

254229 Cheesecake s ovesnými vločkami a ovocem - super na svačinu
Completed: 2 Pages: 1 of 1 Set Completed

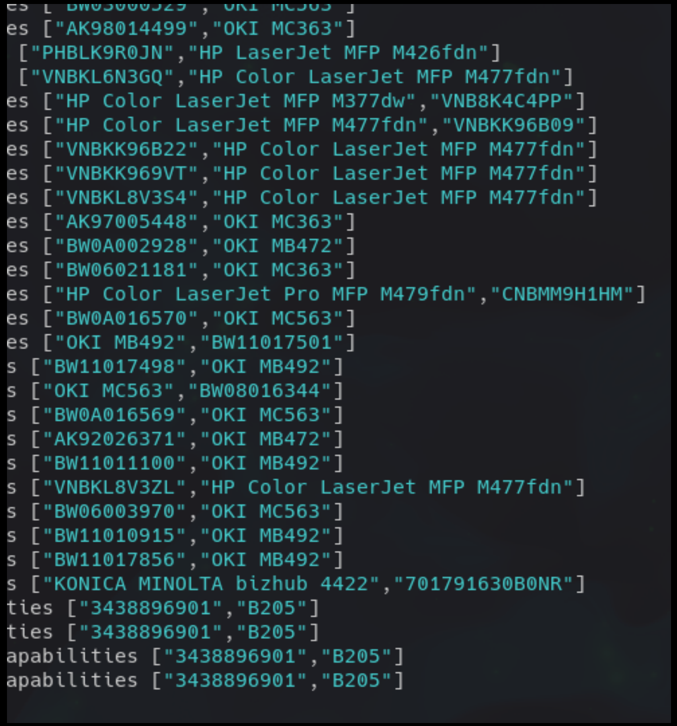
- Default credentials
- View job history, often includes document names which leak sensitive information
- Look for exposed SMB, LDAP, FTP credentials
- Vendor specific configurations and settings that can be abused (export config, exposed serial numbers, resetting)



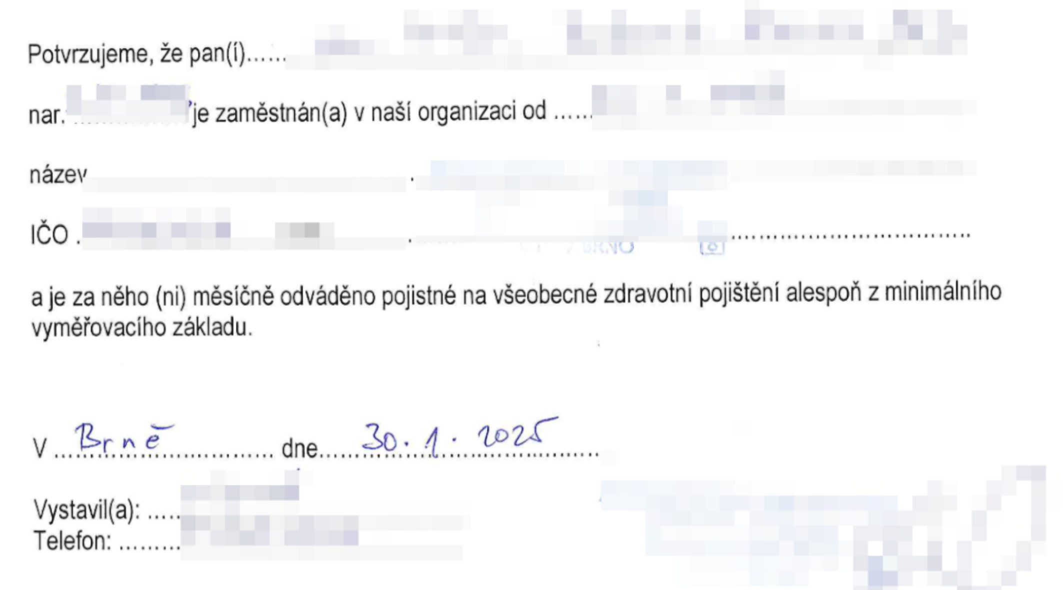
```
<host><data><value></value></data></host>
<directory><data><value>\\FF-D-CESTINA15.ucn.muni.cz\Sharp</value></data></directory>
<username><data encodingMethod="encrypted2"><value>Wvj8qcF9DvU2FJY683ALGg==</value></data></username>
<password><data encodingMethod="encrypted2"><value>7cvEzUTOQL1NLku7snJf/g==</value></data></password>
</smb>
```

HTTP Interface - eSCL

- Ports (80,443,9050,631…)
- Perform scans over HTTP - `/eSCL/ScannerCapabilities`
- Information extraction



```
es ["BW03000529","OKI MC563"]
es ["AK98014499","OKI MC363"]
 ["PHBLK9R0JN","HP LaserJet MFP M426fdn"]
 ["VNBKL6N3GQ","HP Color LaserJet MFP M477fdn"]
es ["HP Color LaserJet MFP M377dw","VNB8K4C4PP"]
es ["HP Color LaserJet MFP M477fdn","VNBKK96B09"]
es ["VNBKK96B22","HP Color LaserJet MFP M477fdn"]
es ["VNBKK969VT","HP Color LaserJet MFP M477fdn"]
es ["VNBKL8V3S4","HP Color LaserJet MFP M477fdn"]
es ["AK97005448","OKI MC363"]
es ["BW0A002928","OKI MB472"]
es ["BW06021181","OKI MC363"]
es ["HP Color LaserJet Pro MFP M479fdn","CNBMM9H1HM"]
es ["BW0A016570","OKI MC563"]
es ["OKI MB492","BW11017501"]
s ["BW11017498","OKI MB492"]
s ["OKI MC563","BW08016344"]
s ["BW0A016569","OKI MC563"]
s ["AK92026371","OKI MB472"]
s ["BW11011100","OKI MB492"]
s ["VNBKL8V3ZL","HP Color LaserJet MFP M477fdn"]
s ["BW06003970","OKI MC563"]
s ["BW11010915","OKI MB492"]
s ["BW11017856","OKI MB492"]
s ["KONICA MINOLTA bizhub 4422","701791630B0NR"]
ties ["3438896901","B205"]
ties ["3438896901","B205"]
apabilities ["3438896901","B205"]
apabilities ["3438896901","B205"]
```



Potvrzujeme, že pan(í)...... [redacted]

nar. [redacted] je zaměstnán(a) v naší organizaci od ...... [redacted]

název [redacted]

IČO . [redacted] ....

a je za něho (ni) měsíčně odváděno pojistné na všeobecné zdravotní pojištění alespoň z minimálního vyměřovacího základu.

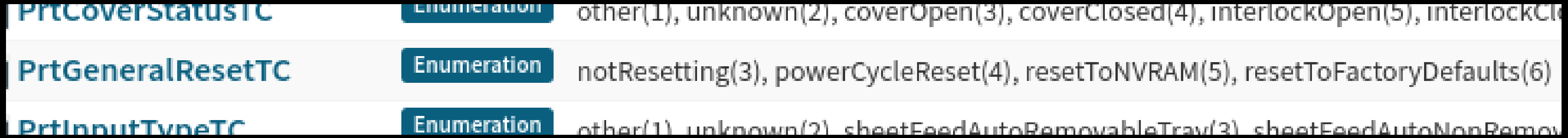
V ...Brně................... dne.......30. 1. 2025.........................

Vystavil(a): ..... [redacted]
Telefon: .... [redacted]

[redacted]

SNMP (161:UDP)

- Community strings (default is often "public" or "private") can be used to gain access to sensitive information
- Version 1 and 2c leak a lot of information about the printer
- SNMPv3 is more secure but can help to identify the printer model and firmware version
- Restart/Reset printer specified in Printer MIB (`1.3.6.1.2.1.43`)



PrtCoverStatusTC	Enumeration	other(1), unknown(2), coverOpen(3), coverClosed(4), interlockOpen(5), interlockCl
PrtGeneralResetTC	Enumeration	notResetting(3), powerCycleReset(4), resetToNVRAM(5), resetToFactoryDefaults(6)
PrtInputTypeTC	Enumeration	other(1), unknown(2), sheetFeedAutoRemovableTray(3), sheetFeedAutoNonRemov

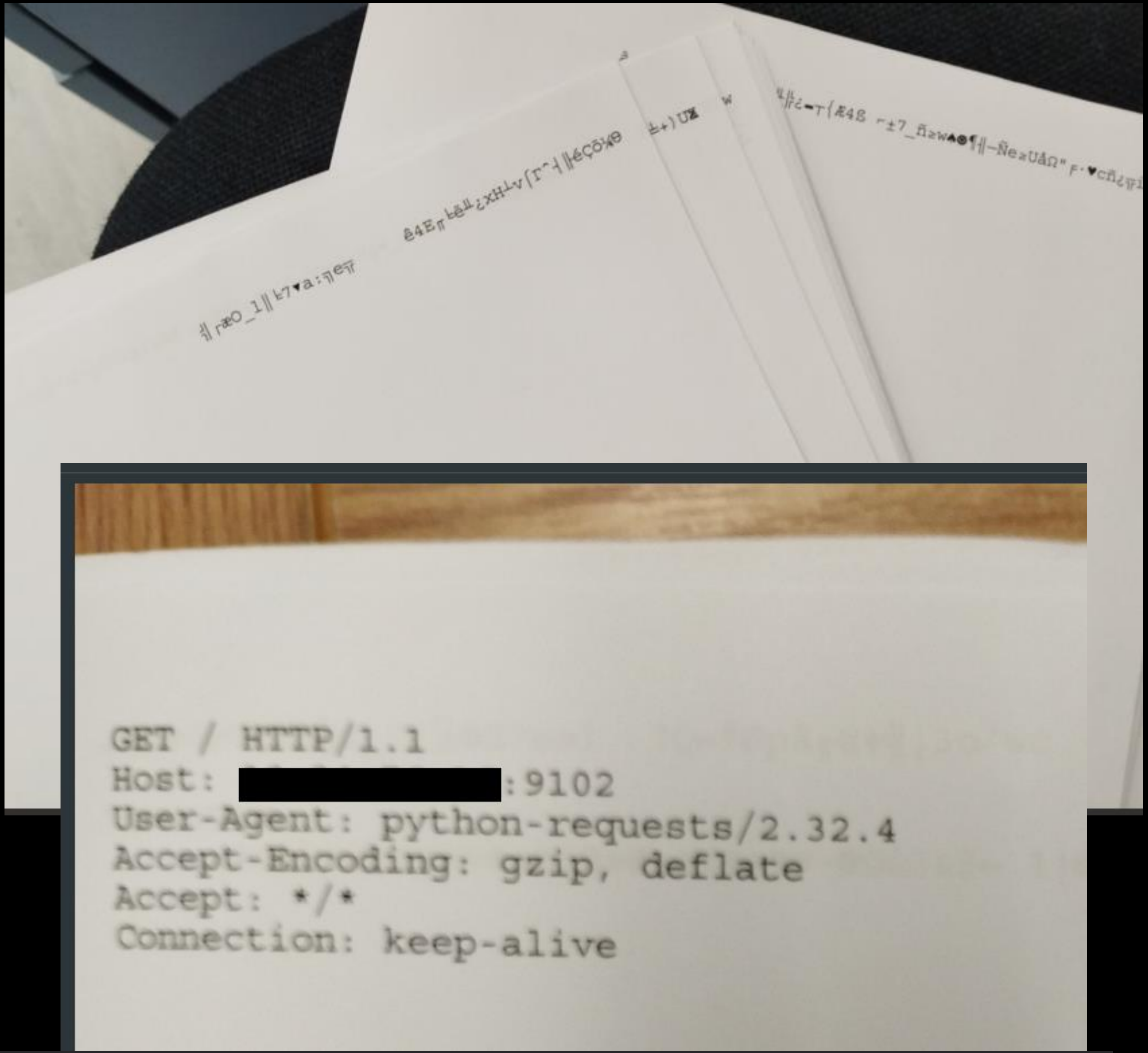
JetDirect (9100:TCP)

- Raw printing
- PostScript, PJL and PCL
- Mostly port 9100, 9100-9110
- Sensitive port
- PRET (ls, cat, touch, reset, info …)

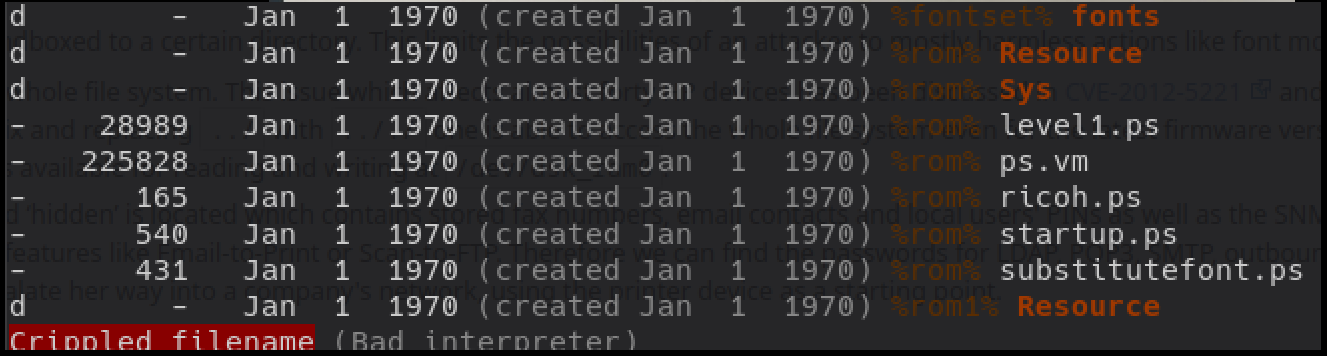
Postscript infinite loop

```
{} loop
```

```
@PJL SET PAPER=A4
@PJL SET COPIES=10
@PJL ENTER LANGUAGE=POSTSCRIPT
```



```
GET / HTTP/1.1
Host: [redacted]:9102
User-Agent: python-requests/2.32.4
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```



```
d        -   Jan  1  1970 (created Jan  1  1970) %fontset% fonts
d        -   Jan  1  1970 (created Jan  1  1970) %rom% Resource
d        -   Jan  1  1970 (created Jan  1  1970) %rom% Sys
-    28989   Jan  1  1970 (created Jan  1  1970) %rom% level1.ps
-   225828   Jan  1  1970 (created Jan  1  1970) %rom% ps.vm
-      165   Jan  1  1970 (created Jan  1  1970) %rom% ricoh.ps
-      540   Jan  1  1970 (created Jan  1  1970) %rom% startup.ps
-      431   Jan  1  1970 (created Jan  1  1970) %rom% substitutefont.ps
d        -   Jan  1  1970 (created Jan  1  1970) %rom1% Resource
Crippled filename (Bad interpreter)
```

Other ports

- LPD (515) Job manipulation
- IPP (631) Same as LPD over HTTP
- Telnet (23)
- Vendor specific (50001 SOAP – Konica, 9050 eSCL -Kyocera)

Resources

- hacking-printers.net
- Rapid7 research
- Tool PRET
- Blog posts
- https://www.blackhat.com/docs/us-17/thursday/us-17-Mueller-Exploiting-Network-Printers.pdf

Other devices

Any questions?