MIDNIGHT BLUE

Rick de Jager, Carlo Meijer

Dialing into the Past

RCE via the Fax Machine

Because Why Not?

Who are we?

Rick de Jager

Freelance researcher, CTF enjoyer,
researcher at Midnight Blue

Carlo Meijer

Founding partner - Midnight Blue

Acknowledgement

35C3
DEF CON 26
Eyal Itkin, Yaniv Balmas - What the Fax?!
Checkpoint Security Research

MIDNIGHT BLUE

Why do this?

Why do this?

- Oday competition
- Targets published 3 months in advance
- Different categories
  - Desktop software
  - Automotive
  - IoT

https://www.zerodayinitiative.com/blog/2024/7/16/announcing-pwn2own-ireland-2024

MIDNIGHT BLUE

Why do this?

ZDI blog

We're also excited to announce a special challenge for this year's contest we're calling the "SOHO Smashup" (as in Small Office/Home Office). This is a real-world scenario of how a threat actor would exploit a home office, so we wanted to include it here, too. It works like this; a contestant picks a router and begins by exploiting the WAN interface. They must then pivot into the LAN to their choice of second target – one of the other devices in the contest. For example, you could pick the TP-Link router and the HP printer. If you compromise both, you'll win $100,000 and 10 Master of Pwn points.

MIDNIGHT BLUE

Why do this?

- Printers have a large attack surface (later)
- We can choose a harder target to avoid duplicates with other teams
- Strategy: choose a reasonably cheap one with encrypted firmware image → competition drawn towards others

Target	Cash Prize
HP Color LaserJet Pro M479fdw	$20,000 (USD)
Lexmark MC3224i	$20,000 (USD)
Canon imageCLASS MF743Cdw	$20,000 (USD)

MIDNIGHT BLUE

Meet our protagonist

- Pwn2Own target since 2021
- Exploited by us ‘22,’ 23, ‘24
- Yocto-linux based
- Fairly decent security posture

+ Fax support!

MIDNIGHT BLUE

Why do this?

Fax Machines
© 1846-1999

Rick de Jager
© 1999-2024

https://www.ebay.co.uk/itm/276701686839?customid=&toolid=10050

MIDNIGHT BLUE

Plan of the attack

Plan of the attack

- Obtain the firmware
- Get some debugging capability
  - JTAG / GDB
- Find vulnerable code
- Exploit the vulnerability
- Get p2o ca$h
- Repeat over fax, give cool CCC talk

MIDNIGHT BLUE

Obtaining firmware

From Lexmark's website:

```
user@bluelagoon:/tmp$ binwalk CXLBL.081.215.fls

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
7716693       0x75BF55        MySQL ISAM index file Version 1
29499865      0x1C221D9       XAR archive, version: 28769, header size: 14349, TOC compressed: 11467389281180270267, TOC un
40569430      0x26B0A56       StuffIt Deluxe Segment (data): f
65470945      0x3E701E1       gzip compressed data, ASCII, has header CRC, last modified: 2068-04-23 16:49:31 (bogus date)
99970506      0x5F56DCA       LANCOM OEM file
134925613     0x80ACD2D       Nagra Constant_KEY IDEA_Key: 10192431 F614728B 643F945F
```

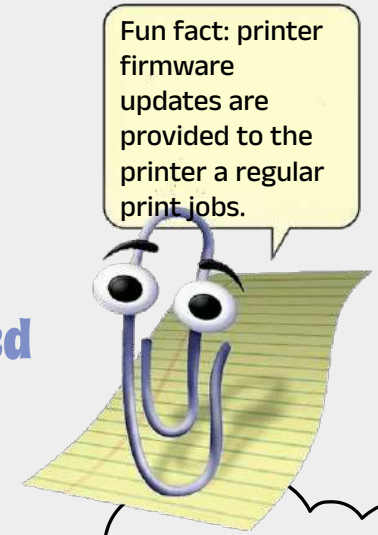
```
user@bluelagoon:/tmp$ ent CXLBL.081.215.fls
Entropy = 7.999999 bits per byte.

Optimum compression would reduce the size
of this 151816071 byte file by 0 percent.

Chi square distribution for 151816071 samples is 267.31, and randomly
would exceed this value 28.56 percent of the times.

Arithmetic mean value of data bytes is 127.4911 (127.5 = random).
Monte Carlo value for Pi is 3.141488502 (error 0.00 percent).
Serial correlation coefficient is 0.000103 (totally uncorrelated = 0.0).
```

It's encrypted



MIDNIGHT BLUE

Obtaining firmware

Back of my car

MIDNIGHT BLUE

Obtaining firmware

Seller

Are you sure you want to buy this printer?

The toners are running low. If you want to print you'll have to buy new ones soon and they're expensive.

Me

Of course. Why wouldn't I be?

Printing? Why would I want to do that?

MIDNIGHT BLUE

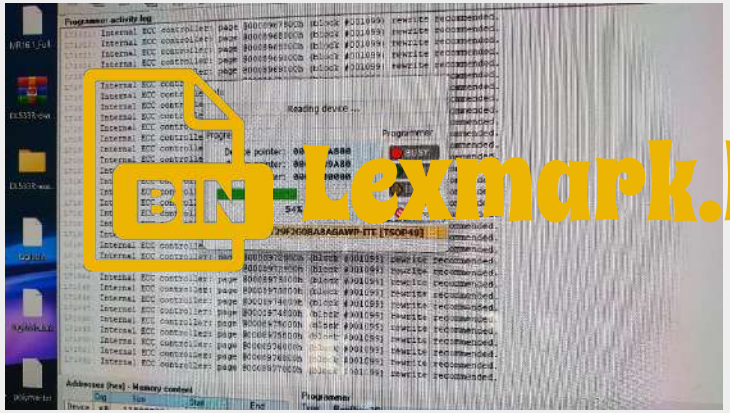
Obtaining firmware

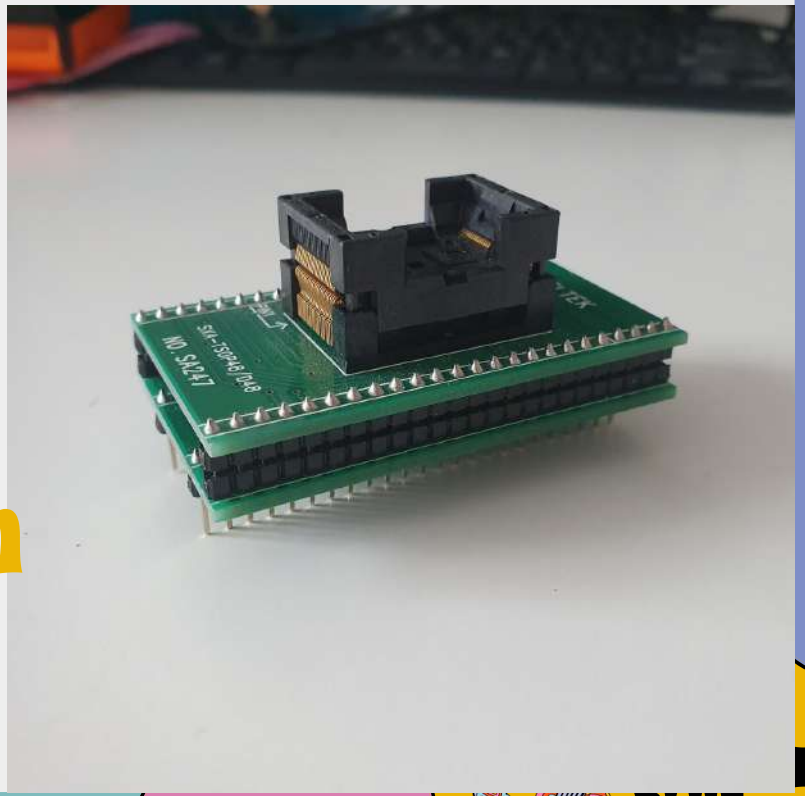
- PCB has markings for JTAG
- We can debug the device with this
  - Set break points
  - Dump the firmware
  - Modify instructions in RAM

- Seems to talk, spit out the IDCODE (ARM Ltd.)
- After a day of tinkering, we gave up :/

Obtaining firmware

- The more hard-core approach
- De-solder the NAND flash from the PCB
- Put it in a universal reader/programmer
- Patch the reader software so that it accepts our cheap TSOP48 adapter from eBay





Lexmark.bin

Obtaining firmware

```
user@bluelagoon:/tmp$ /usr/local/bin/ubireader_display_info ubi.bin
UBI File
--------------------
        Min I/O: 2048
        LEB Size: 126976
        PEB Size: 131072
        Total Block Count: 1986
        Data Block Count: 1079
        Layout Block Count: 2
        Internal Volume Block Count: 1
        Unknown Block Count: 904
        First UBI PEB Number: 104

        Image: 0
        --------------------
                Image Sequence Num: 0
                Volume Name:Kernel
                Volume Name:Base
                Volume Name:Copyright
                Volume Name:Engine
                Volume Name:InternalStorage
                Volume Name:MBR
                Volume Name:ManBlock
```

```
user@bluelagoon:/tmp/ublfs-root/ubi.bin$ unsquashfs img-0_vol-Base.ubifs
Parallel unsquashfs: Using 16 processors
11164 inodes (12690 blocks) to write

[=============================================================|] 12690/12690 100%

created 10284 files
created 842 directories
created 870 symlinks
created 0 devices
created 0 fifos
created 0 sockets
```

Name	Size	Modified
bin	95 items	6/13/19 at 10:27 PM
boot	0 items	6/13/19 at 10:28 PM
dev	0 items	5/27/18 at 3:27 AM
etc	147 items	6/13/19 at 10:28 PM
home	5 items	6/13/19 at 10:16 PM
lib	79 items	6/13/19 at 10:28 PM
media	0 items	5/27/18 at 3:27 AM
mnt	0 items	5/27/18 at 3:27 AM
opt	3 items	6/13/19 at 10:28 PM
pkg-netapps	2 items	6/13/19 at 10:27 PM
proc	0 items	5/27/18 at 3:27 AM
run	0 items	5/27/18 at 3:27 AM
sbin	94 items	6/13/19 at 10:28 PM
srv	0 items	5/27/18 at 3:27 AM
sys	0 items	5/27/18 at 3:27 AM
tmp	0 items	5/27/18 at 3:27 AM
usr	9 items	8/10/18 at 8:10 AM
var	15 items	12/5/18 at 5:21 PM
Build.Info	941 B	6/13/19 at 10:27 PM
web	*0 B*	*4/12/19 at 9:41 PM*

MIDNIGHT BLUE

Obtaining firmware

- Soldered back the NAND
- Works

MIDNIGHT BLUE

Initial access

Initial access

- Device has secure boot
- Can't just modify the NAND flash
- Need an exploit to get low level access
- 💡 Can use published P20 vulnerability[1]

[1] https://www.nccgroup.com/us/research-blog/analyzing-a-pjl-directory-traversal-vulnerability-exploiting-the-lexmark-mc3224i-printer-part-2/

MIDNIGHT BLUE

Initial access

```
user@bluelagoon:~$ ssh -i id_rsa root@10.12.0.20
Last login: Wed Dec 18 17:16:46 2024 from 10.12.0.2
root@ET788C77107F14:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ET788C77107F14:~#
```

- Can upload and run GDB
- Can now debug vulns
- Of course: update fw and lose shell

MIDNIGHT BLUE

Attack surface

Protocols	CGI scripts	File formats	PDF filters	Font types
HTTP(S)	allfaxerrlogs	image/jpeg	EexecDecode	Type1
LPD	allfaxlogs	image/gif	ASCII85Decode	TrueType
IPP	auto-fwdebug-se	image/png	ASCIIHexDecode	MMType1
Fax	basic_auth.cgi	image/bmp	CCITTFaxDecode	Type3
AppSocket/9100	ccs_logs.cgi	image/x-portable-bitmap	DCTDecode	Type0
	ccs_logs_datagen	image/x-portable-graymap	LZWDecode	CIDFontType0
	ccs_reset.cgi	image/x-portable-pixmap	RunLengthDecode	CIDFontType0C
	ccs_se.cgi	image/x-portable-anymap	NullDecode	CIDFontType2
	ceres_se	image/tiff	PDFDecrypt	CIDFontType2C
	cndlog	image/pcx	FlateDecode	
	collect-selogs-cgi	image/dcx	ReusableStreamDecode	
	datacapture	application/pdf	GIFDecode	
	dcsdebug	application/postscript	PNGDecode	
	del_input_cap		BMPDecode	
	directed_discovery.sh		Base64Decode	
	download_input_cap		SwapBitOrder	
	enginedebugdata		PCXDecode	
	epbbdebug		SubFileDecode	
	eventlogdebug_se		ImageRGBDecode	
	eventlog_se		ImageGrayDecode	
	exportfile		JPXDecode	
	...		JBIG2Decode	

MIDNIGHT BLUE

Attack surface

Protocols	CGI scripts	File formats	PDF filters	Font types
HTTP(S)	allfaxerrlogs	image/jpeg	EexecDecode	Type1
LPD	allfaxlogs	image/gif	ASCII85Decode	TrueType
IPP	auto-fwdebug-se	image/png	ASCIIHexDecode	MMType1
Fax	basic_auth.cgi	image/bmp	CCITTFaxDecode	Type3
AppSocket/9100	ccs_logs.cgi	image/x-portable-bitmap	DCTDecode	Type0
	ccs_logs_datagen	image/x-portable-graymap	LZWDecode	CIDFontType0
	ccs_reset.cgi	image/x-portable-pixmap	RunLengthDecode	CIDFontType0C
	ccs_se.cgi	image/x-portable-anymap	NullDecode	CIDFontType2
	ceres_se	image/tiff	PDFDecrypt	CIDFontType2C
	cndlog	image/pcx	FlateDecode	
	collect-selogs-cgi	image/dcx	ReusableStreamDecode	
	datacapture	application/pdf	GIFDecode	
	dcsdebug	application/postscript	PNGDecode	
	del_input_cap		BMPDecode	
	directed_discovery.sh		Base64Decode	
	download_input_cap		SwapBitOrder	
	enginedebugdata		PCXDecode	
	epbbdebug		SubFileDecode	
	eventlogdebug_se		ImageRGBDecode	
	eventlog_se		ImageGrayDecode	
	exportfile		JPXDecode	
	...		JBIG2Decode	

ZDI-24-405

ZDI-22-333

ZDI-22-330
ZDI-22-331
ZDI-22-332
ZDI-23-668
ZDI-23-669
ZDI-24-084

ZDI-22-328
ZDI-22-382
ZDI-23-663
ZDI-23-664
ZDI-23-666
ZDI-24-081
ZDI-24-083

ZDI-24-082

MIDNIGHT BLUE

Timeline

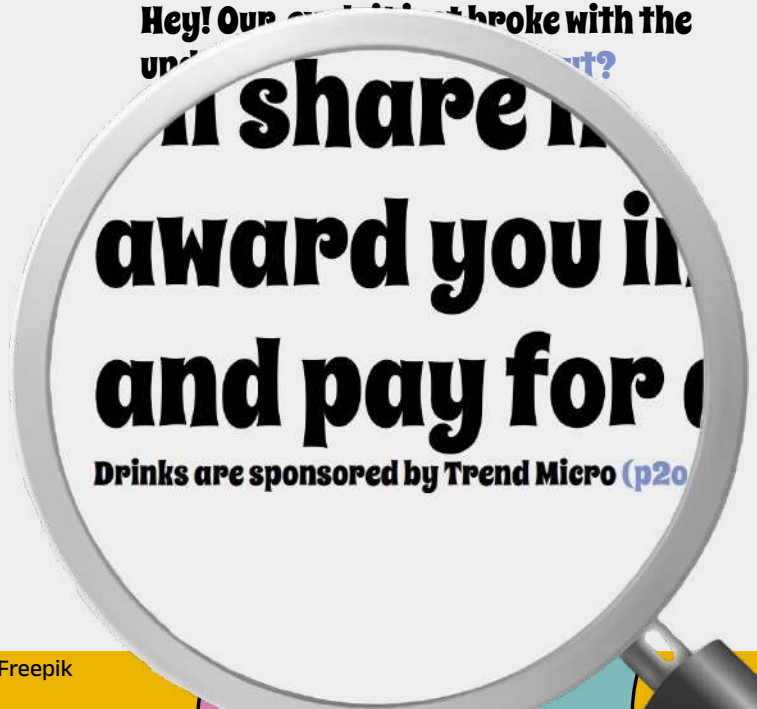
- 2022
  - We dumped nand, developed a decryptor
  - Developed a file format exploit (jp2k)
  - First stage (router) exploit failed on stage :(
- 2023
  - Developed another jp2k exploit
  - A new update drops hours before the signup deadline
    - It contains entirely new crypto
    - ... and rollback prevention

MIDNIGHT BLUE

Saved by @bl4sty

@rdjgr

Hey! Our [illegible] broke with the [illegible]rt?



@bl4sty

Sure! Let me know I can do for you

What's in it for me?

Sounds good!

Timeline (cont'd)

- 2023
  - Developed another jp2k exploit
  - A new update drops hours before the signup deadline
    - It contains entirely new crypto
    - ... and rollback prevention
  - Exploit is successful 🥳
- 2024
  - We and @bl4sty merge into PHP Hooligans
  - @bl4sty gets mad, breaks WTM and releases new decryptor[1]
  - We drop 2 more exploits 🥳

[1] https://github.com/blasty/lexmark/

MIDNIGHT BLUE

JBIG2 image compression

- Reachable over both pdf and fax
- Roll-your-own decoding library
- Plan: exploit pdf, get p2o ca$h, port to fax

MIDNIGHT BLUE

JBIG2 image compression

SUCCESS - Our final attempt of Pwn2Own Ireland is confirmed! PHP Hooligans / Midnight Blue (@midnightbluelab) used an integer overflow to exploit the Lexmark printer and play us a tune. They earn $10,000 and 2 Master of Pwn points.

[REDACTED]

Still under embargo

https://m.media-amazon.com/images/I/21eALQdHYYL._UX250_.jpg

MIDNIGHT BLUE

JBIG2 Heap feng-shui

Without building an entire CPU

- JBIG2 is actually great for heap shaping
  - Elastic size elements
  - Alloc / Free at will
- Sprayed data can be G4 compressed
- Extensions are your friend
  - Clean, controlled allocation
  - Easy to implement
- Every segment has function pointers

```
struct jbig2_extension_details_t __packed
{
    int32_t type;
    char* data;
    int32_t size;
};
```

```
struct segment __packed
{
    uint32_t segment_number;
    enum SEGMENT_TYPE type;
// ... < snip > ...
    void* func_read_header;
    void* func_dump;
    void* func_decode;
    void* func_free;
    void* data;
};
```

JBIG2 Heap feng-shui

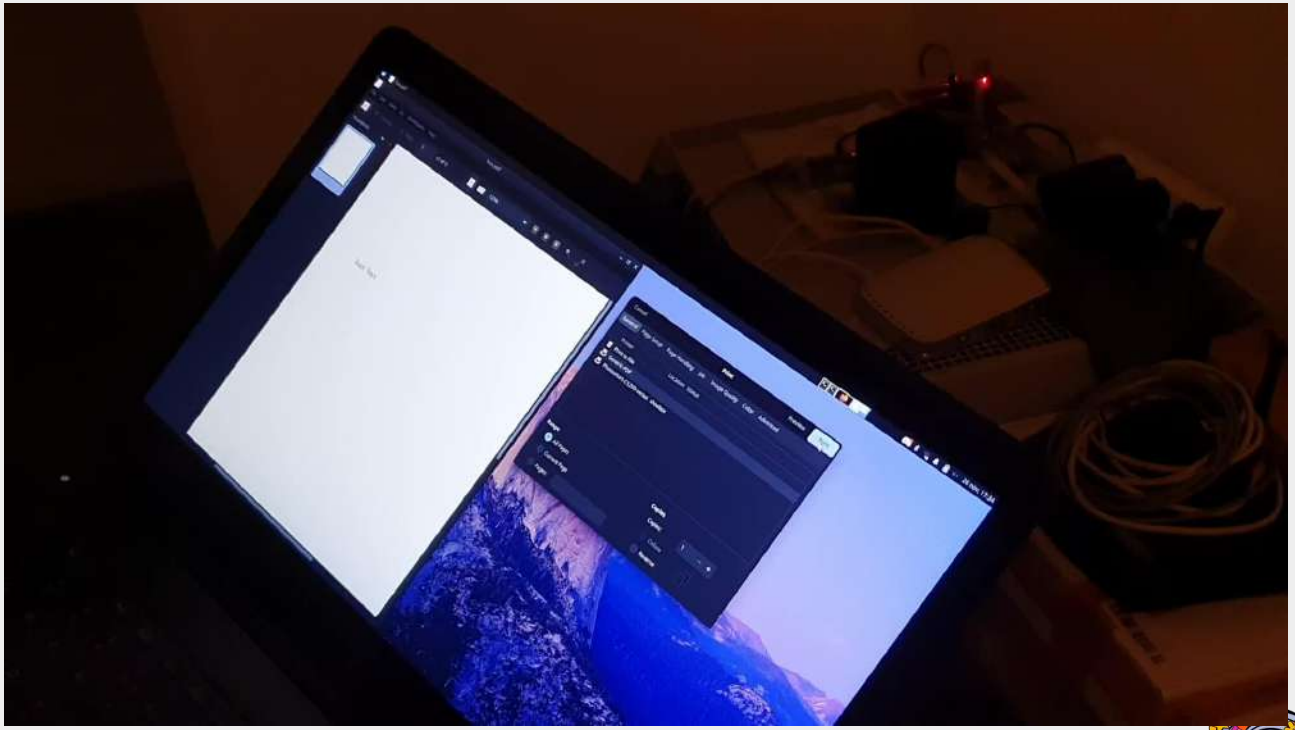
```python
def main():
    exp = Exploit()
    exp.add_comment(1337, b"Hello 38C3!")
    data = exp.dump()
```

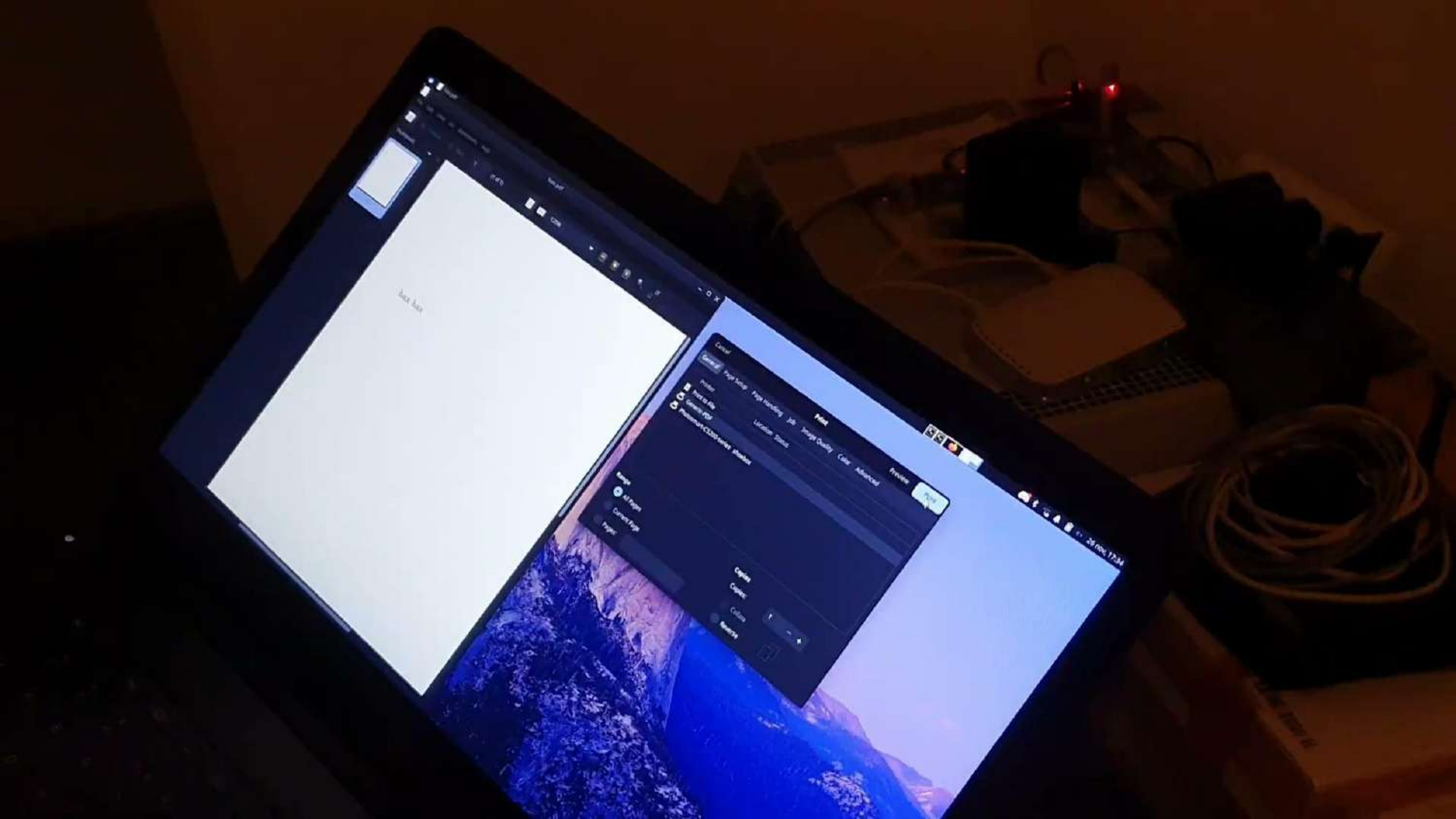
```
 1337  page=0  offset=000e size=17     EXTENSION
          0, 0 ref_segments:
Hello 38C3!
```

```
pwndbg> hexdump 0x221a0
+0000 0x0221a0  |...9|....|....|....|
+0010 0x0221b0  |..He|llo.|38C3|!...|
```

MIDNIGHT BLUE

Exploit time





Exploit time

MIDNIGHT BLUE

Fax

Intermezzo: analog phones

- Who here has an analog phone line?
- Good for you. We don't
- How do we even test this?
- Came across this puppy

https://campingpower.nl/ziggo-connextbox-wifi-uit-gaan-wifi-uit/

MIDNIGHT BLUE

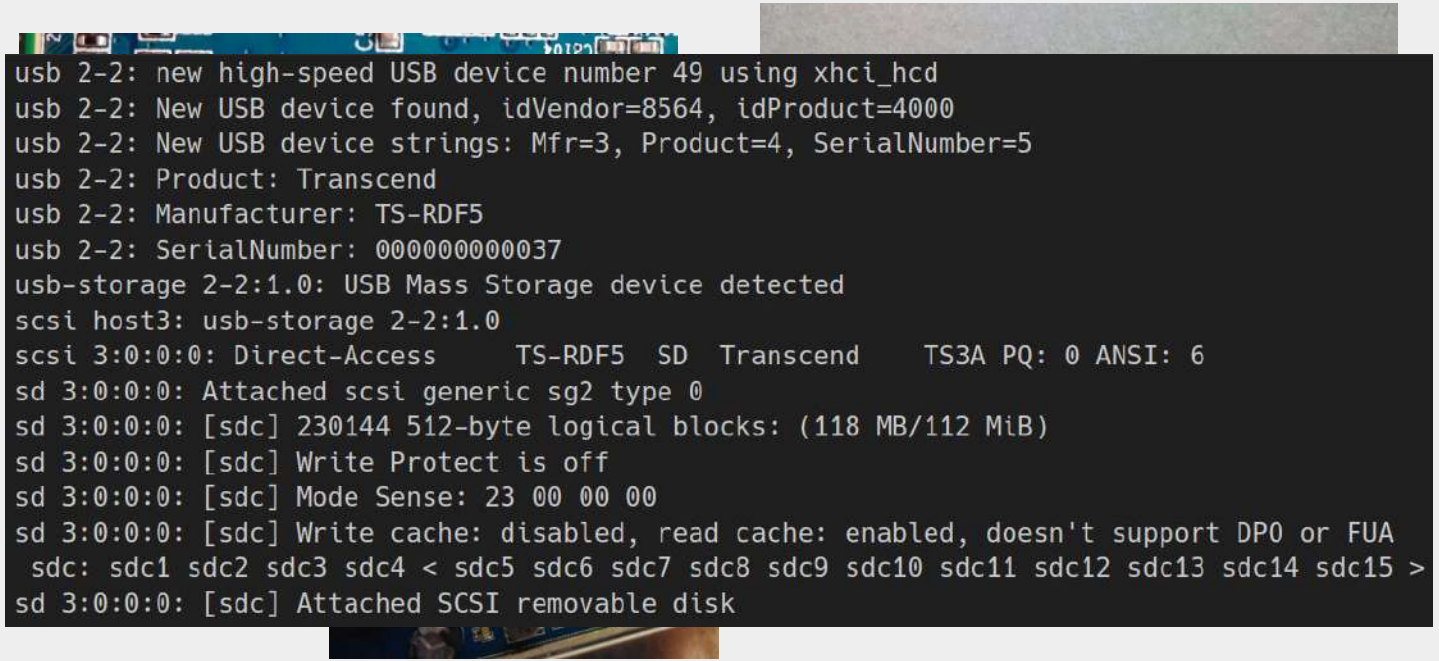
Intermezzo: analog phones

- Phone via cable ISP
- Otherwise unusable
- Unless...

https://www.olx.pl/d/oferta/router-connect-box-ziggo-CID9[illegible]DXZ[illegible].html

MIDNIGHT BLUE

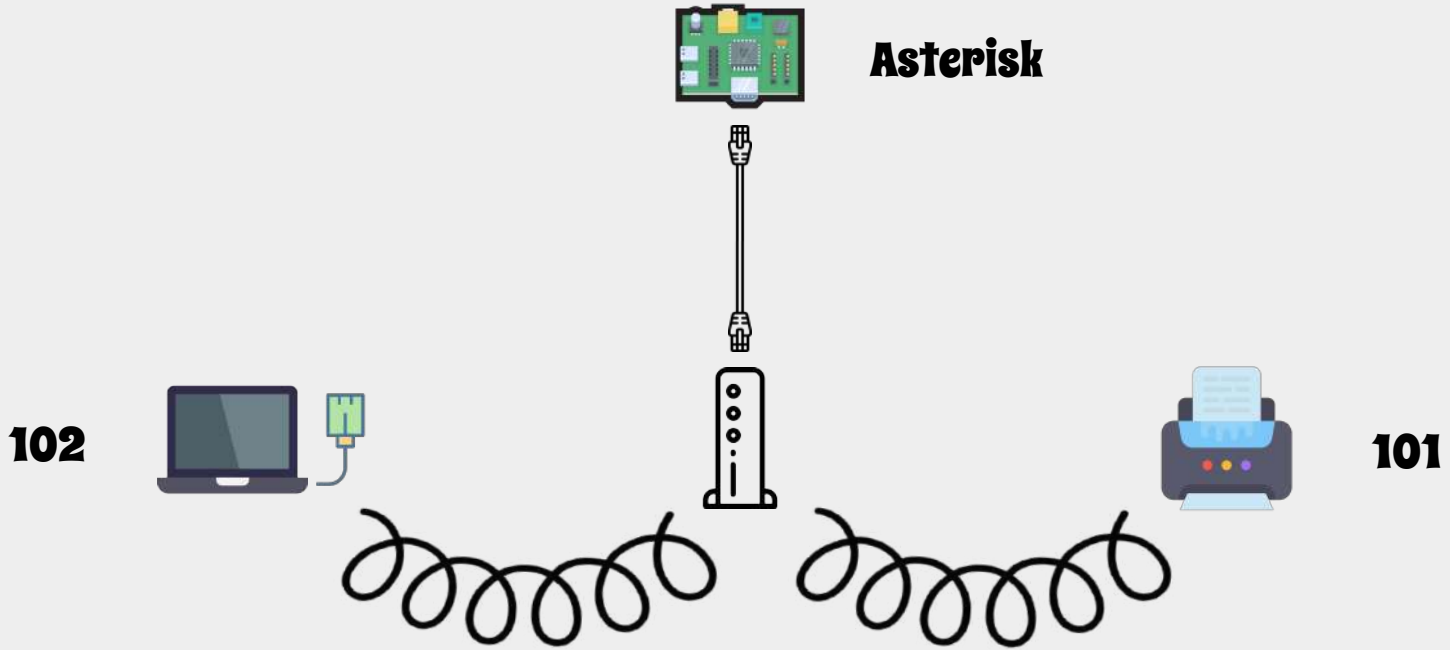
Cable ISP modem



https://blog.danman.eu/about-adding-a-static-route-to-my-docsis-modem/

MIDNIGHT BLUE

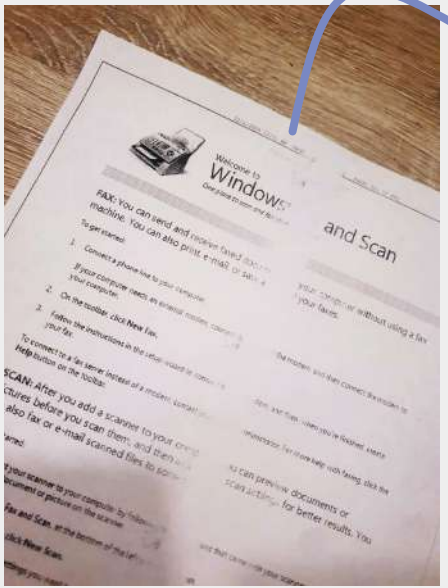
The setup



https://www.flaticon.com/free-icon/{file}
file = {ethernet_3826471, spring_14526364, lead_16373305, laptop_595528, paper_10216243, modem_236787}

MIDNIGHT BLUE

Today we sent a fax



Fax sent with the setup

MIDNIGHT BLUE

Fax

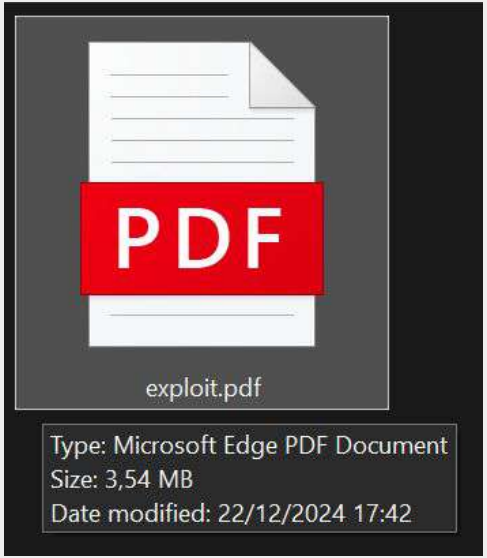
ITU standard	Released date	Data rates (bit/s)	Modulation method
V.27	1988	4800, 2400	PSK
V.29	1988	9600, 7200, 4800	QAM
V.17	1991	14400, 12000, 9600, 7200	TCM
V.34	1994	28800	QAM
V.34bis	1998	33600	QAM
ISDN	1986	64000	4B3T / 2B1Q (line coding)

https://en.wikipedia.org/wiki/Fax

MIDNIGHT BLUE

... so just fax the exploit?

- Fax speeds are not great for heap shaping
- Pwn2Own exploit is 3.5 MB
  - _just_ 1.7h @ 4800bps 😅
  - Rewrite the exploit from scratch
- Lexmark's JBIG2 is non-standard
  - Nobody else supports this format



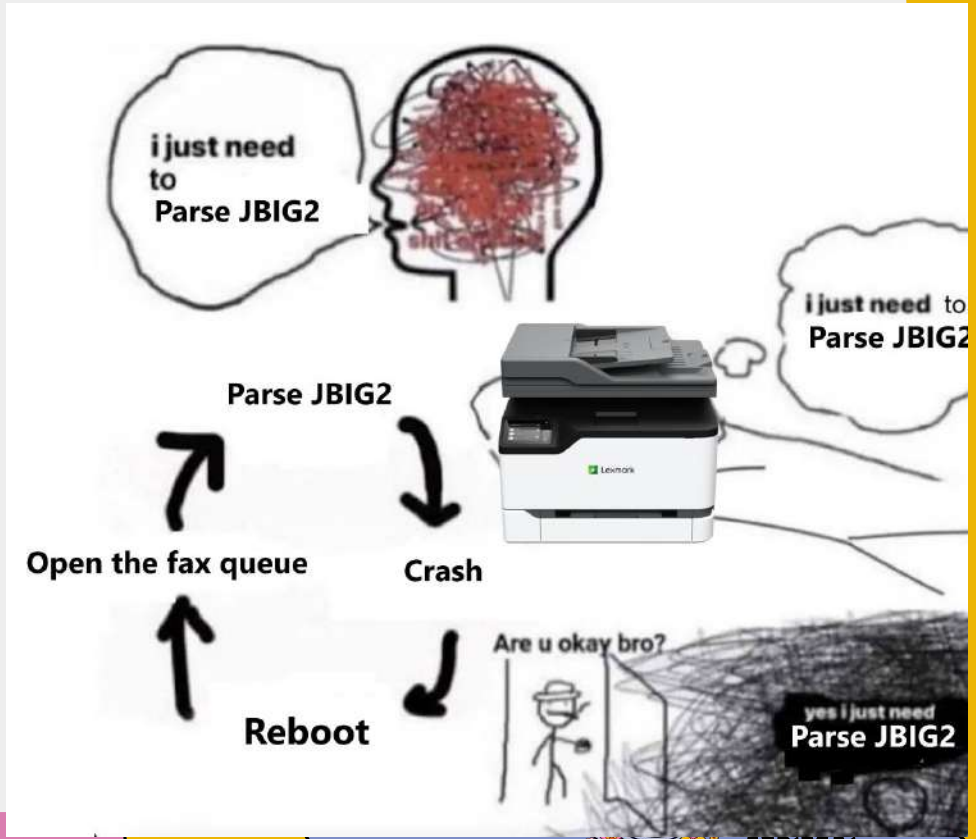
MIDNIGHT BLUE

So I wrote a fax client

- I patched efax[1]
  - raw data support
  - Send NSF to enable JBIG2
  - No Error Correction Mode, yolo

- High stakes faxing
  - Faxes are saved on disk
  - any parser error crashes the printer
  - The printer reboots on crash

  ⇒ Instantly bootlooped



[1] https://www.cce.com/efax/

Now what?

Who uses fax?

- Healthcare
  - Patient records, prescriptions, other sensitive medical documents.
  - 89% of medical offices, 70% of healthcare organizations rely on fax.[1]
- Real Estate
  - Send and receive purchase agreements, lease agreements, other.
  - “Faxes help facilitate the sale of properties and ensure that all parties involved in a transaction are on the same page.”
- Government and Legal
  - Widely used within government agencies, courts, and legal practices.
  - 63% of legal departments use faxes to transmit sensitive documents (2019).
  - Some government agencies and courts may require faxes.
- Finance and Banking
  - Sometimes required for signing documents.

[1]https://www.linkedin.com/pulse/why-we-still-using-fax-machines-healthcare-jack-kreeter
https://blog.thegrizzlylabs.com/2023/03/what-industries-still-rely-on-faxes.html

MIDNIGHT BLUE

Attacker POV

Pros

- Large attack surface
- No firewalls or NIDS
- High-profile targets
- Wiretap phone line
- Extremely easy to monetize
- Peek printed documents
- Pivot into internal network
    - ARP spoof, PtH, fax on AD domain
- Often overlooked

Cons

- Fragmented landscape
- Need device fingerprint
- Not scalable

MIDNIGHT BLUE

Demo time

Thanks!

Any questions?

Rick de Jager
@rdjgr
rick@bricked.tech
https://bricked.tech

Carlo Meijer

c.meijer@midnightblue.nl
https://midnightblue.nl

MIDNIGHT BLUE