

Malware in the wild book.

cocomelonc.github.io/book/2023/12/13/malwild-book.html

December 13, 2023

1 minute read

Hello, cybersecurity enthusiasts and white hackers!



Alhamdulillah, I finished writing this book today. It was quite difficult. In sha Allah everything will be fine. O Allah, Lord of the Worlds, give strength to all children who are fighting for their lives.

Why is the book called that? **MALWILD** - means **Mal**ware in the **Wild**.

I will be very happy if this book helps at least one person to gain knowledge and learn the science of cybersecurity. The book is mostly practice oriented.



DECEMBER 2023

MALWILD

zhassulan zhussupov

@cocomelonc

```

defined (ECC_CURVE) == (ECC_CURVE == NIST_K163)
    #define coeff_a 1
    #define cofactor 2
    /* NIST-B-163 */
    const gf2elem_t poly_m1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t c1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t base_x = { 0x5c4e3d, 0x4e4e6d5e, 0xaa
    const gf2elem_t base_y = { 0xccdaa3d9, 0x0536d538, 0x32
    const scalar_t base_order = { 0x99f8a5ef, 0xa2e0cc0d, 0x00
    #endif

    #if (ECC_CURVE == NIST_B163)
    #define coeff_a 1
    #define cofactor 2
    /* NIST-B-163 */
    const gf2elem_t poly_m1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t c1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t base_x = { 0x5c4e3d, 0x4e4e6d5e, 0xaa
    const gf2elem_t base_y = { 0xccdaa3d9, 0x0536d538, 0x32
    const scalar_t base_order = { 0x99f8a5ef, 0xa2e0cc0d, 0x00
    #endif

    #if (ECC_CURVE == NIST_B233)
    #define coeff_a 1
    #define cofactor 2
    /* NIST-B-233 */
    const gf2elem_t poly_m1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t c1 = { 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000, 0x00000000 };
    const gf2elem_t base_x = { 0x5c4e3d, 0x4e4e6d5e, 0xaa
    const gf2elem_t base_y = { 0xccdaa3d9, 0x0536d538, 0x32
    const scalar_t base_order = { 0x99f8a5ef, 0xa2e0cc0d, 0x00
    #endif

```



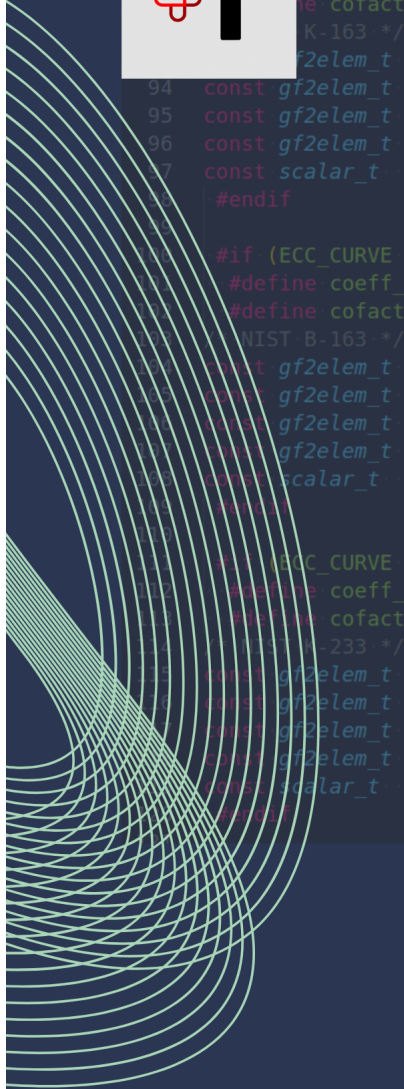
MALWARE DEVELOPMENT TRICKS FROM MALWARE SOURCE CODE LEAKS AND MALWARE ANALYSIS EXAMPLES

LICENSE: FREE (32 USD)



DECEMBER 2023

ALL RIGHTS RESERVED



```
defined (ECC_CURVE) == (ECC_CURVE == NIST_K163)
#define coeff_a 1
#define cofactor 2
/* NIST B-163 */
const gf2elem_t polynomial = { 0x000000c9, 0x00000000, 0x00
94 const gf2elem_t coeff_b = { 0x00000001, 0x00000000, 0x00
95 const gf2elem_t base_x = { 0x5c94eee8, 0xde4e6d5e, 0xaa
96 const gf2elem_t base_y = { 0xccdaa3d9, 0x0536d538, 0x32
97 const scalar_t base_order = { 0x99f8a5ef, 0xa2e0cc0d, 0x00
98 #endif
99
100 #if (ECC_CURVE == NIST_B163)
101 #define coeff_a 1
102 #define cofactor
103 /* NIST B-163 */
104 const gf2elem_t
105 const gf2elem_t
106 const gf2elem_t
107 const gf2elem_t
108 const scalar_t
109 #endif
110
111 #if (ECC_CURVE
112 #define coeff_
113 #define cofact
114 /* NIST B-233 */
115 const gf2elem_t
116 const gf2elem_t
117 const gf2elem_t
118 const gf2elem_t
119 const scalar_t
120 #endif
```



All proceeds from the sale of the book will go to help children from Kazakhstan with cancer.

This book is dedicated to my wife, Laura, and my children, Yerzhan and Munira. Also, thanks to everyone who is helping me through these difficult times. The proceeds from the sale of this book will be used to treat my friends:



Antipin Eleazar, Scaphocephaly (Sagittal Craniosynostosis).



Khasenova Djamilya, Hepatoblastoma (liver cancer).

The book is divided into three logical chapters:

- Malware dev tricks from source code leaks
- Malware analysis examples
- Helper scripts (most in python) for malware analysis

All material in the book is based on my posts from [WebSec blog](#), [HVCK magazine](#), [MSSP Lab blog](#) and [my own articles](#).

If you have questions, you can ask them on my [email](#).

My Github repo: <https://github.com/cocomelonc>

This book costs \$32 but you can pay as much as you want. If you are unable to pay for it, I will send it to you for free.

If you cannot pay via Paypal:



Deposit BTC



Send only BTC to this deposit address.
This address does not support deposit of non-fungible token, please go to NFT page to deposit NFT.

Wallet Address

**1MMDN38mheQn9h2Xa2H6hqMSfF
YKW4nQUE**



Network

Bitcoin



Minimum deposit

0.00000001 BTC

Expected arrival

1 network confirmation

Expected unlock

2 network confirmations

Save Image

Share Address



Trade anywhere!

Download the Binance App

My Referral ID

452549452

BTC address: **1MMDN38mheQn9h2Xa2H6hqMSfFYKW4nQUE**



Deposit ETH



Send only ETH to this deposit address.
This address does not support deposit of non-fungible
token, please go to NFT page to deposit NFT.

Wallet Address

**0xf6ed40f61b603a4b2ac7c0770340
53df4f718f37**



Network

Ethereum (ERC20)



Minimum deposit

0.00000001 ETH

Expected arrival

12 network confirmation

Expected unlock

12 network confirmations

Save Image

Share Address



Trade anywhere!

Download the Binance App

My Referral ID

452549452

ETH address: **0xf6ed40f61b603a4b2ac7c077034053df4f718f37**



Deposit XMR



Send only XMR to this deposit address.
This address does not support deposit of non-fungible token, please go to NFT page to deposit NFT.

Wallet Address

87E2aD7P7FGiQrUdznXPqtH7enHy
wV8qm5kMqKziKLz8ECWZENE8ZV
5JWRTJhA3RVS5rxSogRsd7z7yX2D
Mn29dR3Vfnbj



Network

Monero



Minimum deposit

0.0000001 XMR

Expected arrival

3 network confirmation

Save Image

Share Address



Trade anywhere!

Download the Binance App

My Referral ID

452549452

XMR address:

87E2aD7P7FGiQrUdznXPqtH7enHywV8qm5kMqKziKLz8ECWZENE8ZV5JWRTJhA3RVS5rxSogRsd7z7yX2DMn29dR3Vfnbj

Binance email: zhzhussupovkz@gmail.com

VISA/Mastercard:

4400 4301 3484 3363 AIMAN ANTIPINA (cardholder)

4400 4302 1897 8630 ZHANAR KHASSENOVA (cardholder)

For Kaspi:

+7 700 270 7807 (Айман А.)

+7 701 242 6662 (Алия Ш.)

Charity fund +1 from Kazakhstan (Kaspi QR):



If you are unable to pay for it, I will send it to you for free.

[MALWILD book](#)

| All examples are practical cases for educational purposes only.

Thanks for your time happy hacking and good bye!

PS. All drawings and screenshots are mine