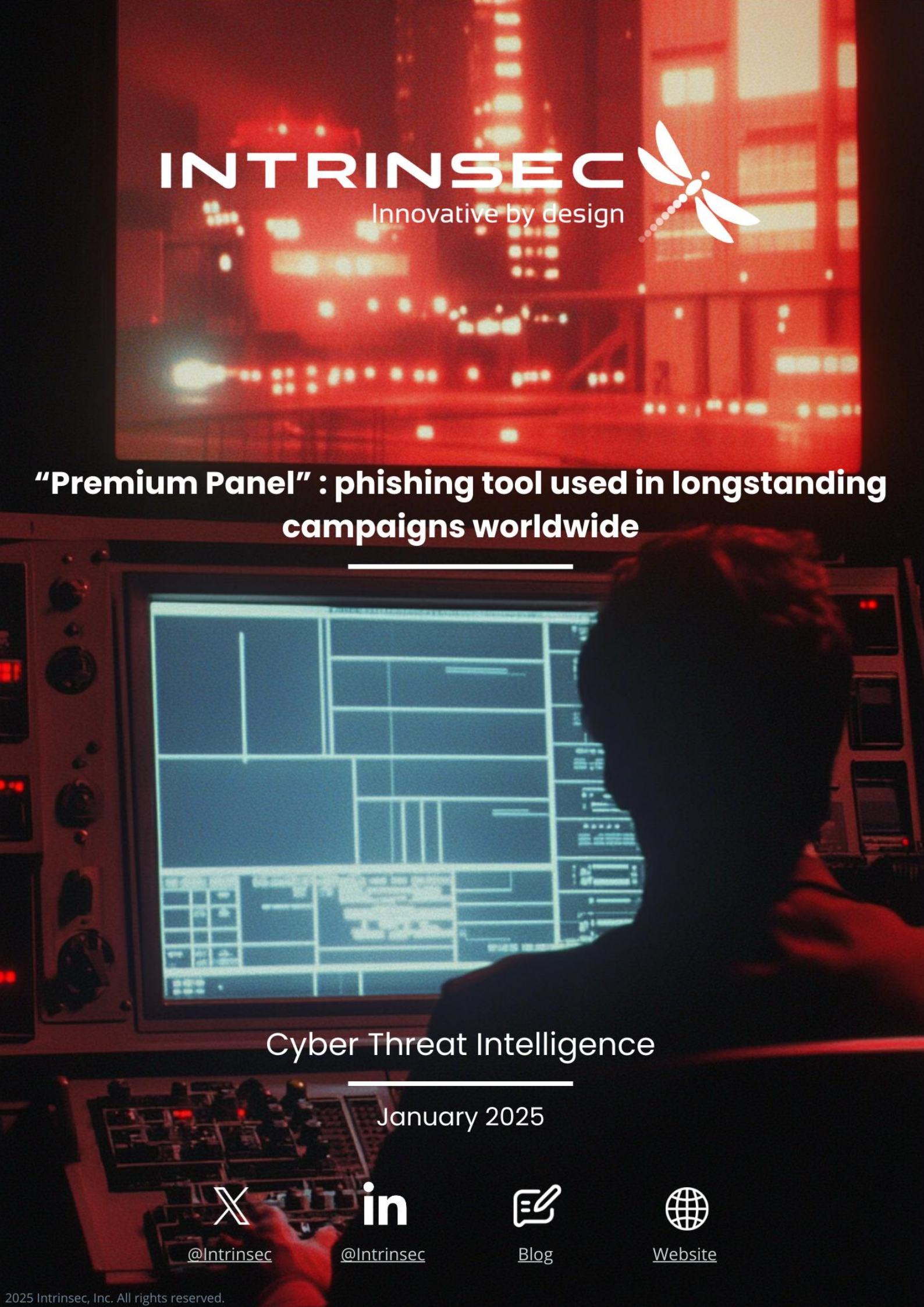


INTRINSEC

Innovative by design

“Premium Panel” : phishing tool used in longstanding campaigns worldwide

Cyber Threat Intelligence

January 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

Key findings

In this report are presented:

- A phishing toolkit that we named "Premium panel", due to the presence of the sentence "Live Control Panel Premium". This toolkit is comprised of a panel composed of multiple .php pages and .js scripts that handle victim credentials logging and redirection to other pages.
- Phishing domains masquerading as login pages from multiple renown companies in various industries, mostly banking and logistics. The companies usurped are mostly Western, with exceptions in Saudi Arabia, Israël, South Africa, Taïwan, Qatar, Guatemala.
- Strategic analysis of the different phishing campaigns that used this toolkit, including companies usurped, sectors and countries targeted.
- Insight into the connection between the phishing domains and the panel used to receive details and credentials from victims. We discovered a method to track new domains linked to the "Premium panel" phishing toolkit. Threat actors used either compromised legitimate domains to host their phishing pages, hosted their websites using temporary/free domain names, or registered domain spoofing the usurped companies' brand. Telegram tokens and id found on unprotected panels can be used to track clusters and threat actors targeting specific countries and industries.

Introduction

Phishing is still the most common initial access vector used by threat actors worldwide. Phishing can be used for a variety of purposes, including credentials harvesting and malware delivery. As far as phishing for credentials is concerned, Intrinsec CTI discovered a phishing toolkit that has been used for at least 2 years. While the author of this toolkit was not identified, we discovered means to track this threat and produce actionable content for defences. Phishing toolkits are still relevant as even low-tier threat actor(s) can easily set them up, which usually inflates the number of campaigns seen in the wild. This is what we observed, as threat actor(s) are using this toolkit, that we named "Premium panel" due to the presence of a specific string, in various campaigns usurping mostly European companies in selected industries.

I. Strategical Intelligence

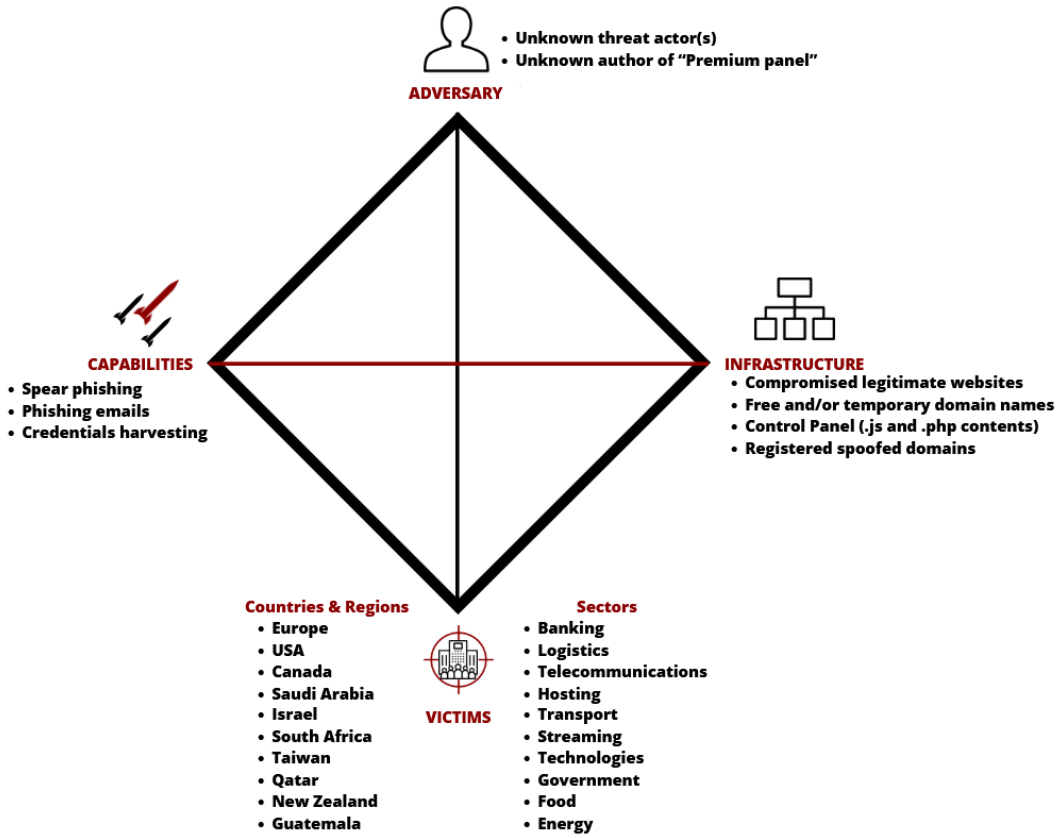


Figure 1: Diamond model analysis of the phishing toolkit analysed.

1. Long standing campaigns observed

Several phishing domains usurping popular companies were setup. After collecting and analysing these domains, we were able to gain more insights into these campaigns.

First, we noticed that same IP addresses were used to host phishing pages, usurping different companies. It is probable that a same threat actor may operate one IP address used for various phishing domains. For instance, the IP address 139.177.180[.]48 was used between May and June 2024 to host domains usurping a bank in Cyprus, and a telecom company in Hungary. The IPs 87.121.221[.]102 and 87.121.221[.]214 were used between March and June 2023 to host domains usurping French telecom and banking companies. The IP 2.59.255[.]11 was used in the beginning of June 2024 to host domains usurping the same companies. In a similar manner, the IP 20.100.169[.]28 was used in September 2023 to host domains usurping the same French telecom and banking companies. The IP 45.55.112[.]74

was used between September 2023 and June 2024 to host domains usurping banking in multiple countries.

Then, we were able to identify the sectors of the different companies usurped, revealing a large exploitation of the Banking sector, followed by the Logistics and Telecom industries. This makes sense if the threat actors leveraging Premium Panel are mainly interested in financial gains. Banking credentials are more valuable in monetary terms as they can be used immediately to extract money. Logistics and Telecom could contain credit cards information and be used for online purchases.

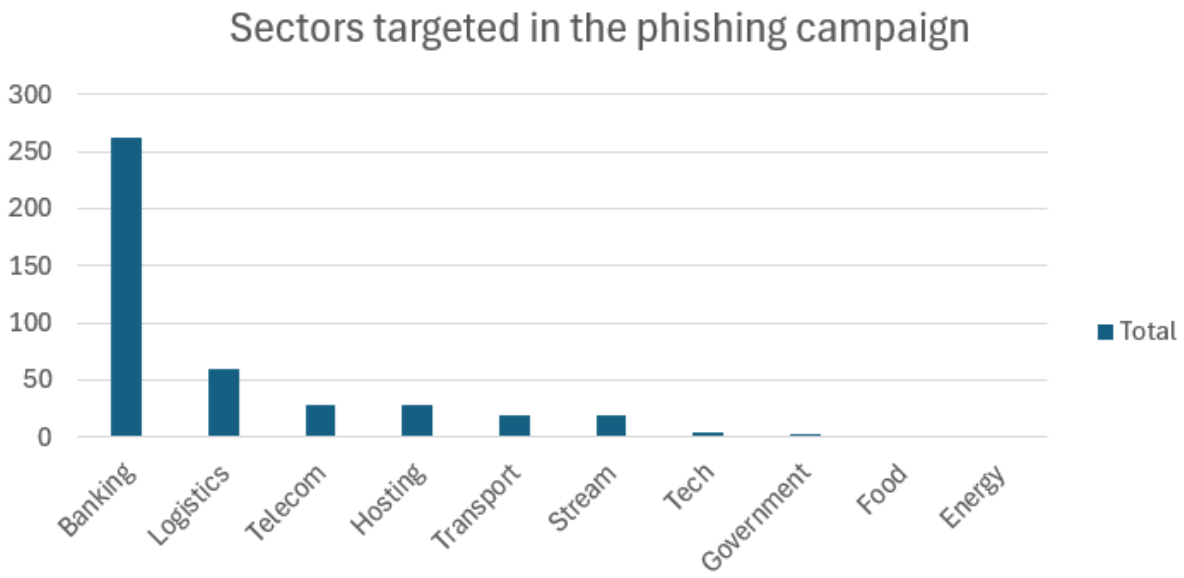


Figure 2: Sectors targeted by phishing domains using the kit.

For the countries of the companies usurped, we noticed that no companies registered in the UK were usurped. However, the phishing pages in English language could also be used to target British citizens. Overall, Western countries were mostly targeted, with exceptions in Saudi Arabia, South Africa, Israël, Taiwan, Qatar, Guatemala.

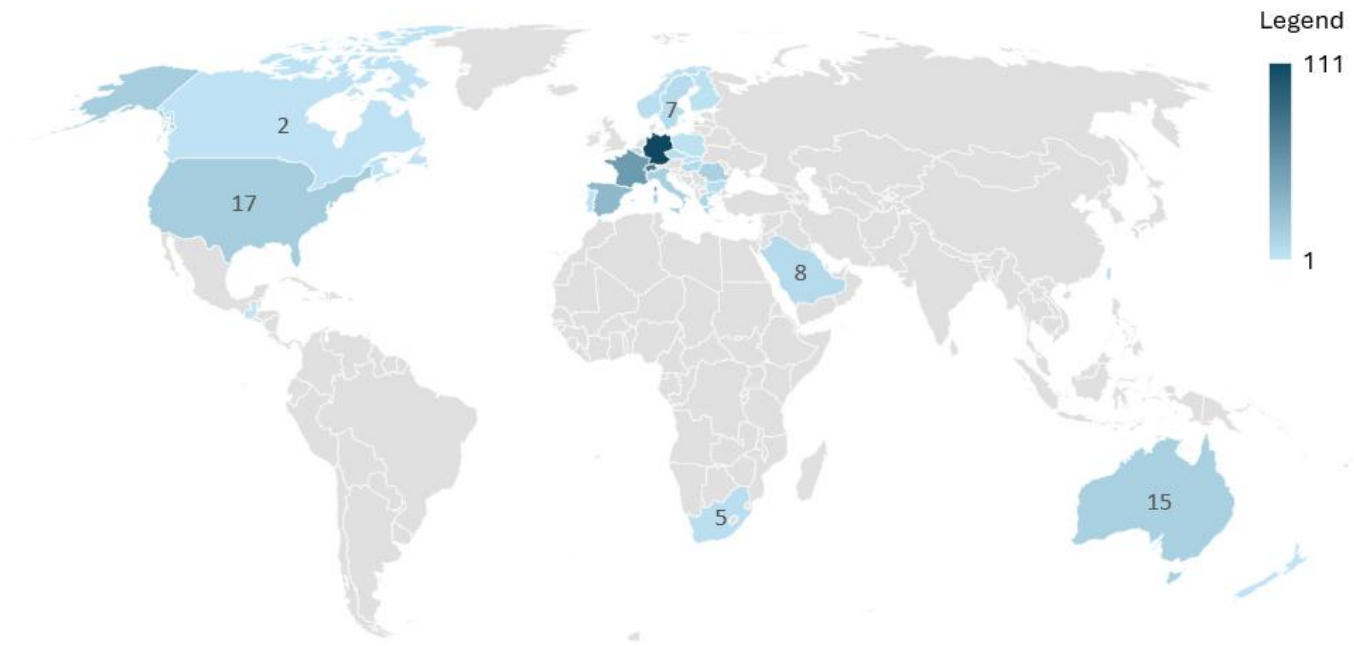


Figure 3: Countries of the companies usurped by domains using the kit.

Lastly, below is a timeline summarizing the evolution of the use of "Premium Panel", detailing the start and end date of the different campaigns.

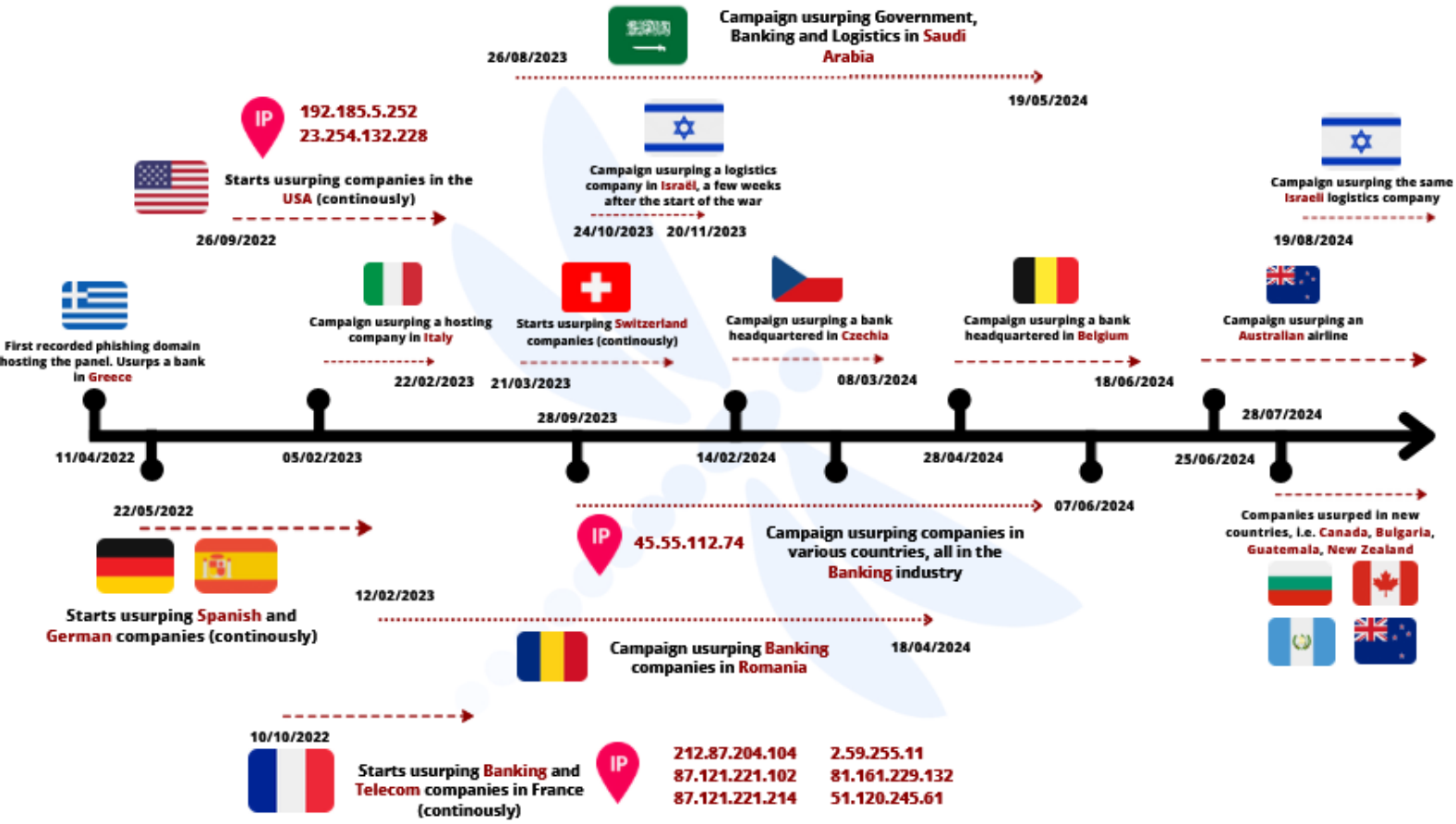


Figure 4: Timeline of the different phishing campaigns using the kit.

2. Attribution

While we did not discover the original threat actor behind this phishing toolkit, we suspect that several different threat actors use it, either by paying it as-a-service, or by copying the .php and .js contents directly from other phishing domains. We did not find mentions of this phishing toolkit in analysis by other cybersecurity editors, but we did however notice that it was mentioned in a Facebook group named "ProDefence", on 23 April 2024. The exact same panel that we discovered is disclosed in this group, accompanied by screenshots and the following message:

"Just another #banking #phishing... or not?!? Live control panel premium >>"Victim not connected"

Redirects > Login error, email, email error, card, card error, SMS, SMS error ..

Looks like a Man-in-the-Middle.... "Premium Panel" An interesting feeling to be inside phishing platforms and see how cyber attacks work. I will come back with more details in a more detailed article! Have fun and stay safe!"

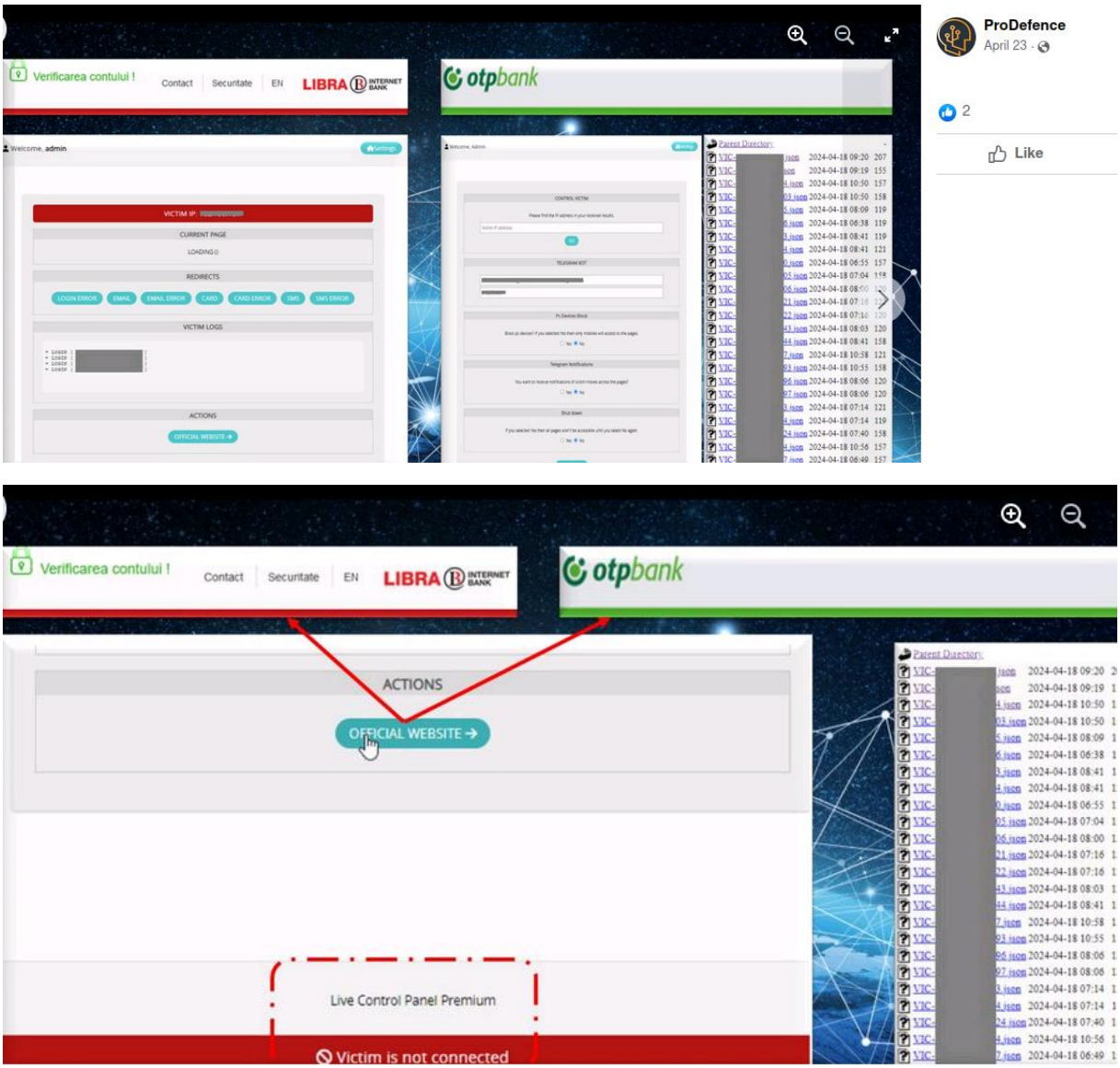


Figure 5: Phishing panel shared by "ProDefence" on Facebook. Source: https://www.facebook.com/story.php/?story_fbid=943071517825105&id=100063667955585

II. Tactical Intelligence

1. Technical analysis

Phishing websites usurping a variety of companies worldwide were leveraged since 2+ years. The websites are copies of the legitimate login pages usurped, while the domains usually do not try to spoof the legitimate companies usurped. Some content of the phishing pages is usually copied by using "href" to the legitimate domains of the company. As such, leveraging Canary tokens could be an effective way to prevent such malicious use of a legitimate website (see Recommendations). In some cases, the content is copied/pasted from the login pages into the phishing pages. Images could also be directly hosted on the phishing domains instead of referencing them from the legitimate domain.

Figure 6: Content from the legitimate websites either copy-pasted or invoked using "href".

Some of the phishing pages are hosted on compromised legitimate websites, while others use solutions to easily host websites or temporary domain names such as codeanyapp[.]com, mybluehost[.]me, cloudwayapps[.]com, mywebsitetransfer[.]com, tempurl[.]host, etc. Some phishing domains spoofed domains of the legitimate companies usurped. In this case, they were registered by the threat actor(s).

2. Processor.php

Viewing the network requests made, we noticed that a file named "processor.php" was requested multiple times and is hosted on the endpoint "/panel/classes" or "/panel/process" of the phishing domains.

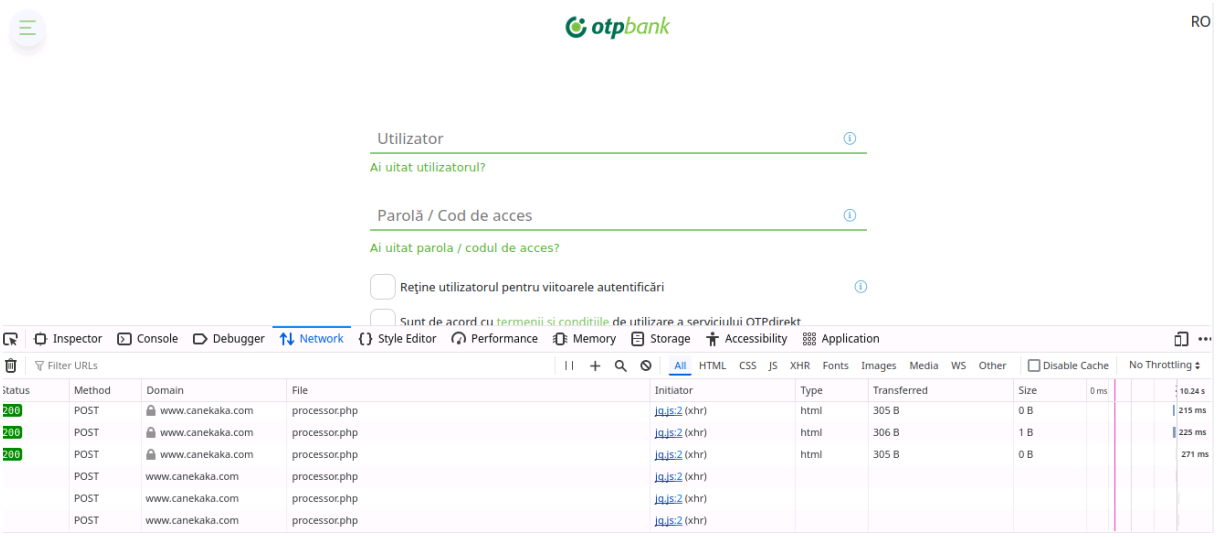


Figure 7: Multiple continuous network requests made to "processor.php".

The file named "processor.php" is the main element used to establish a link between the victim browser and the panel, handling redirection and keeping-alive the connection via a JavaScript installed in the phishing domains. In this script, we see that the variable object "targets" is defined with several keys that were identified as being redirections (see Premium access to the control panel). 1 correspond to "login.php", 2 to "email.php" and so on. A first "setInterval" function is defined and posts data to "processor.php" to "keepAlive" the connection to the "LOGIN" page every 500 milliseconds, which explains the multiple network requests when viewing the phishing domain.

```
    <script src="../panel/res/jq.js"></script>
    <script>

    var targets = {1:"login.php?e=ERROR", 2:"email.php", 3:"email.php?e=ERROR",4:"payment.php",5:"payment.php?e=ERROR",
     6:"sms.php", 7:"sms.php?e=ERROR",8:"done.php", 9:"exit.php" };

    clearRedirections();

 setInterval(function(){
    $.post("../panel/classes/processor.php",
    {keepAlive:1, page:"LOGIN "} );
}, 500);
```

Figure 8: Redirection targets and keepalive functions of the script.

The second setInterval() function also sends a request to processor.php with the data {redirectionListener:1}. The server's response (data) is stored in the variable redirect (value of 0 by default). If the value of redirect is not 0 (redirect==0), it triggers a redirection (window.location=targets[redirect]), which navigates the victim to one of the URLs in the targets object based on the redirect value.

The clearRedirections() function makes a POST request to processor.php with {clearRedirection:1}. This could be used to reset or clear any previous redirection commands, perhaps to prevent multiple redirects.

```
var redirect=0;
setInterval(function(){
    $.post("../panel/classes/processor.php",{redirectionListener:1}, function(data){
        redirect=data;
        if(redirect==0){
            return false;
        }else{
            clearRedirections();
            window.location=targets[redirect];
        }
    });
}, 500);


function clearRedirections(){
    $.post("../panel/classes/processor.php",
    {clearRedirection:1});
}
```

Figure 9: Further interactions of the script with "processor.php".

3. Infrastructure Analysis

3.1 Premium access to the control panel

The login page to the control panel usually looks like this, with mentions of "Live Control Panel – log in":

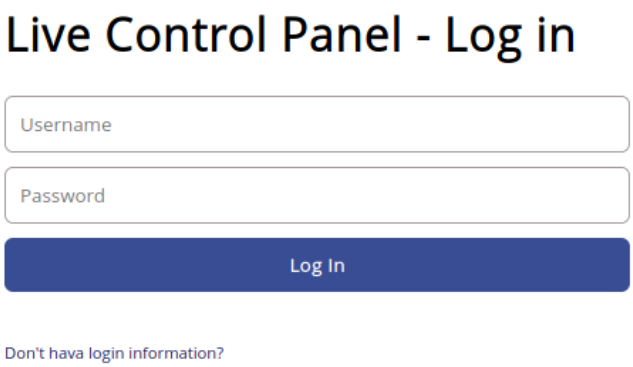


Figure 10: Live Control Panel login page.

However, on some domains, we noticed that the panel was accessible and not protected by login. It appears that by default, the panel is reachable at the endpoint "/panel/settings.php". The panel contains a "Welcome, Admin" message at the top left and various editable settings. A first box named "Control Victim" is used to search for a victim IP address. The second option "Telegram Bot" is used to set the details of a Telegram bot/channel to receive notifications when a victim visits the phishing domain. The option "¨Pc Devices Block" is used to restrict the phishing domain to mobile users only. The option "Telegram notifications" is used to enable/disable notifications when a victim "moves across the pages". And the option "Shut Down" is used to restrict access to the phishing domain. The panel also displays the string "Live Control Panel Premium" at the bottom of the page, which may reveal information about the toolkit.

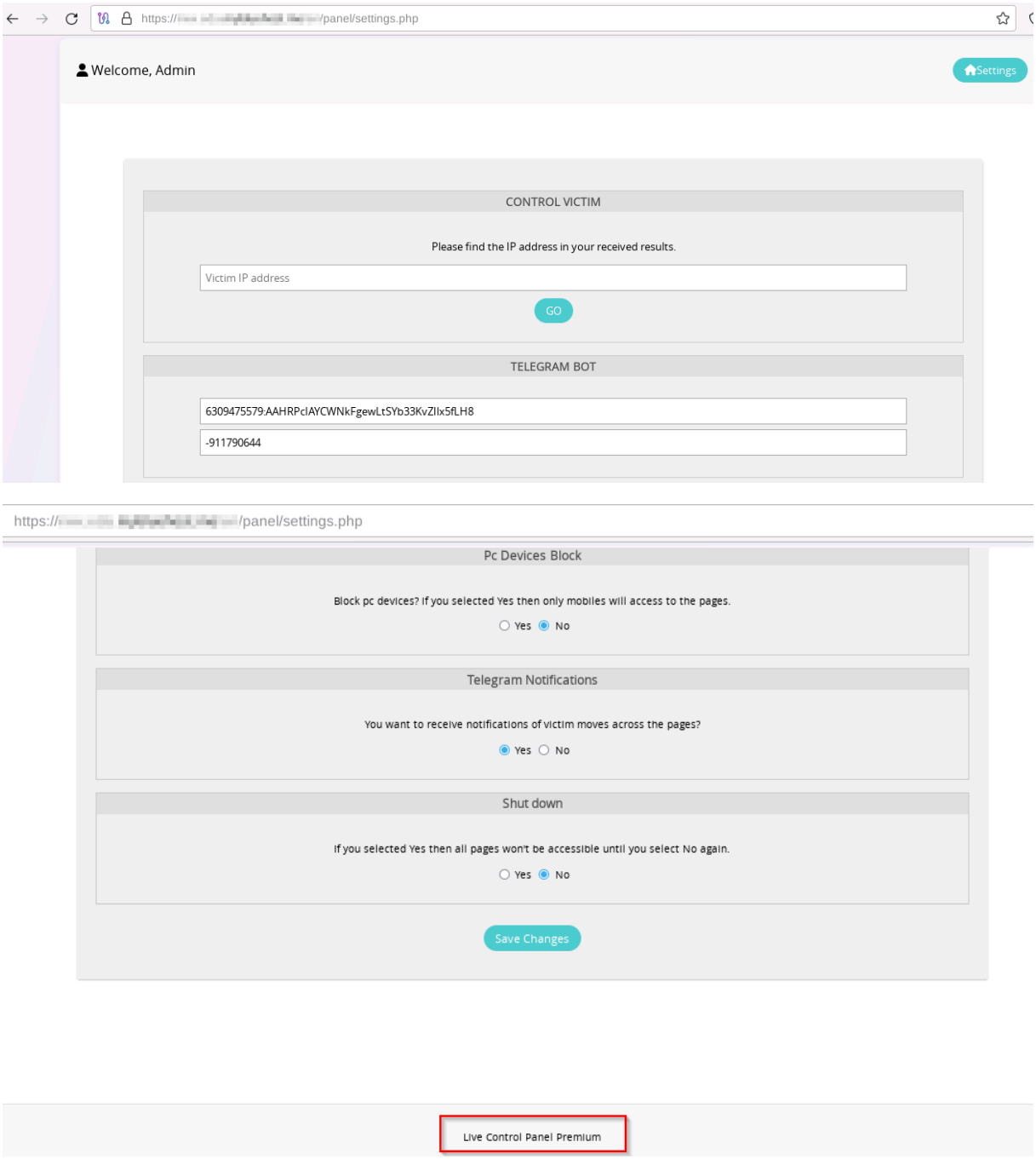


Figure 11: Content of "settings.php" showing the landing page of the phishing kit's panel.

When searching for a victim IP on the panel, we are redirected to a different page "view.php" containing various settings. First, it displays the IP address of the victim, circled in green if it is still connected to the phishing page, or in red if it is not connected anymore. The section "current page" displays the page the victim is currently viewing. "Redirects" contains clickable buttons that redirect the victim's browser to other pages of the phishing domain. "Victim logs" contains the text inputs of the victim. Finally, "Actions" contains a single button

“official website” that redirects the victim browser to the official website of the company usurped.

Figure 12: Actions possible once a victim is connected to the phishing domain.

For example, clicking on the button “SMS” when inside the panel will redirect our browser to “sms.php”. This new page asks the victim for an SMS code, hence the button name “sms”.

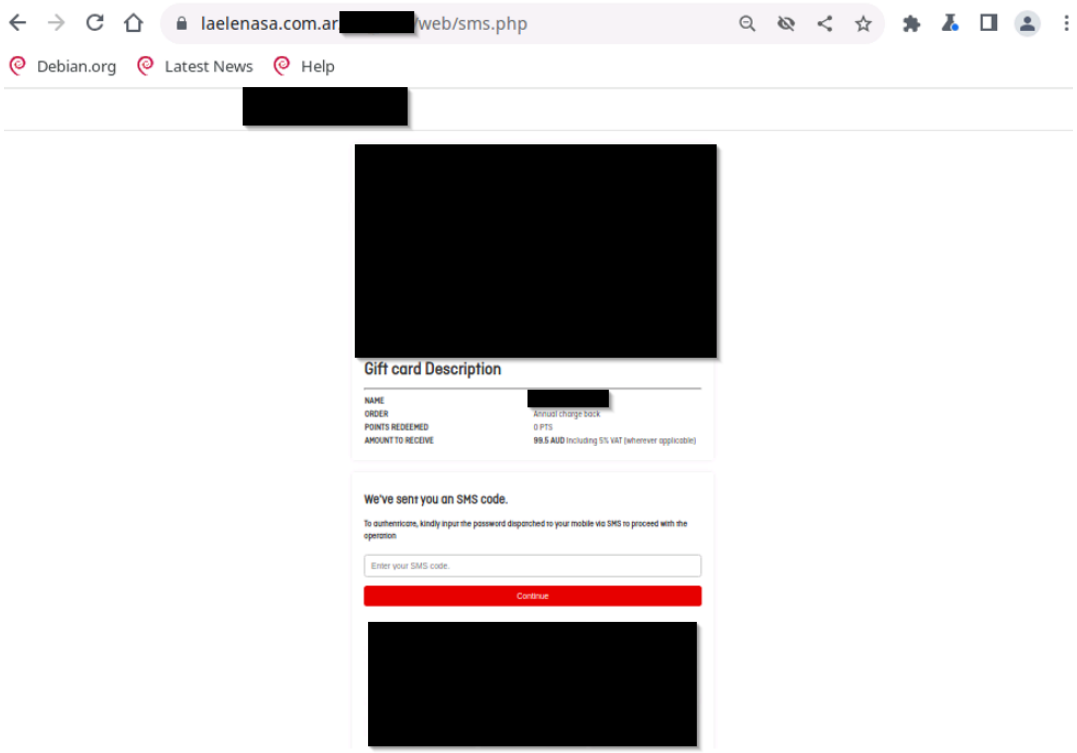


Figure 13: Redirection to “sms.php”.

Clicking on “official website” while the victim is still connected will redirect to the legitimate website of the company usurped, after being redirected to “exit.php”.

Below is an illustrated summary of our findings on how the panel and website interact with each other, and with the victim’s browser.

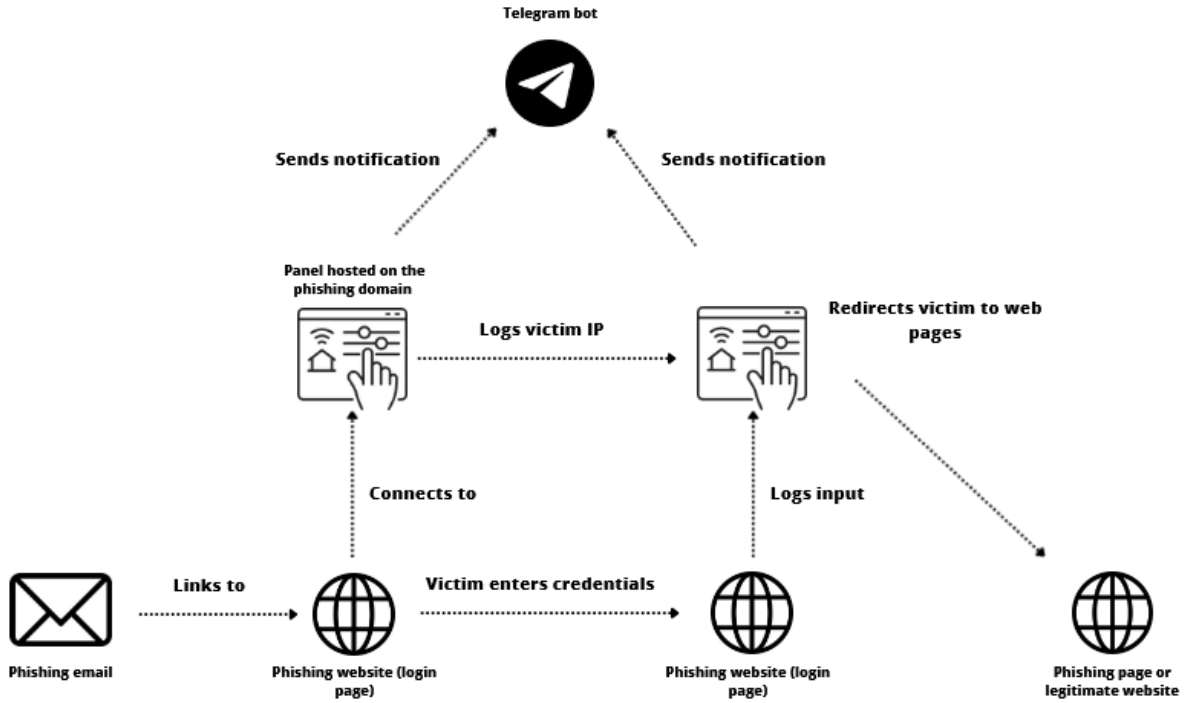


Figure 14: Summary of the interactions between the phishing domain and the panel.

3.2 Additional pivots

Searching for the phishing domains on URL scan, we discovered a method to track them. Querying for the file "jq.js" hosted on "**/panel/res/jq.js**" returns us only the phishing domains that uses "Premium panel".

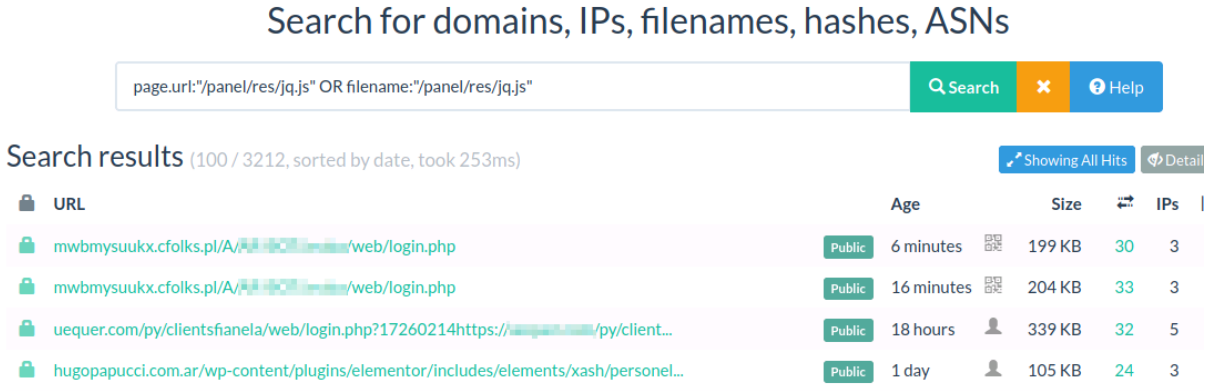


Figure 15: Query to track phishing domains that uses the phishing kit. Source: https://urlscan.io/search/#page.url%3A%22panel%2Fres%2Fjq.js%22%20OR%20filename%3A%22panel%2Fres%2Fjq.js%22

Interestingly, we can also pivot on the IP addresses and mail addresses shared by two or more "Premium panel" phishing domains to discover more phishing domains. For some domains, the mail addresses used to register them were in cleartext in historical WhoIs records using DomainTools. As such, we can discover phishing domains potentially registered by the same individual(s).

For instance, the mail address "tamazpam[@]yahoo[.]com" was used to register a bunch of phishing domains mostly usurping French banking companies. Some of them were confirmed to host the "Premium panel" toolkit, while others were not. The IP address 185.221.67[.]30, used for a "Premium panel" phishing domain usurping an Israeli logistics company was used to host a lot of other phishing domains not related to "Premium panel".

3.3 Telegram

As evidenced on the panel section, some of the users of the phishing toolkit have setup Telegram bots to receive notification. On the unprotected panel, as the token of the bot is visible on some occasions, we can get the Telegram name of the bot using the Telegram API. Collecting all bots visible on the phishing panels could be used to map different clusters with targeted countries/companies/industries.

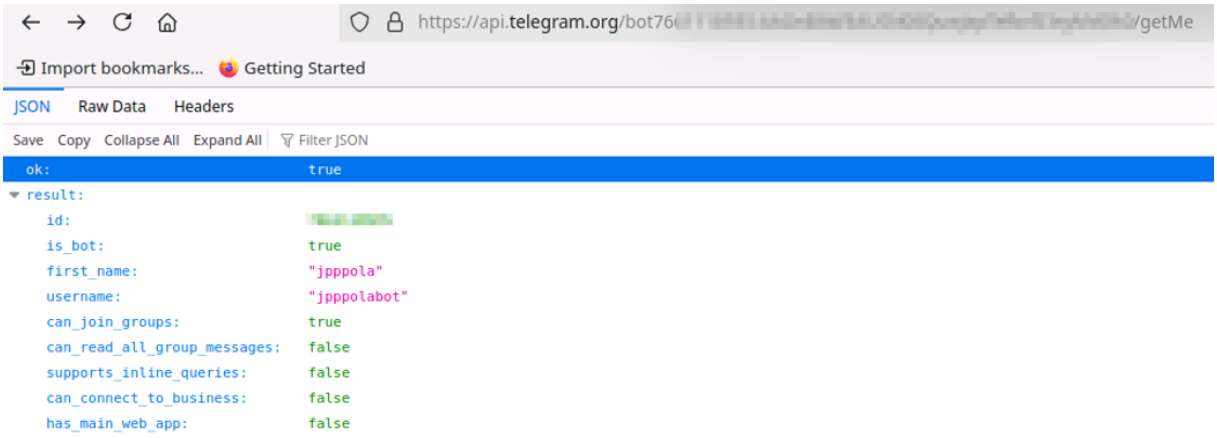


Figure 16: Recovering the Telegram bot connected to the phishing panel using the Telegram API and the bot token.

It is also possible to get the administrator of the bot, by using the ID found on the second line of the phishing panel. Querying the Telegram API with the right parameters returns us the username of the administrator.

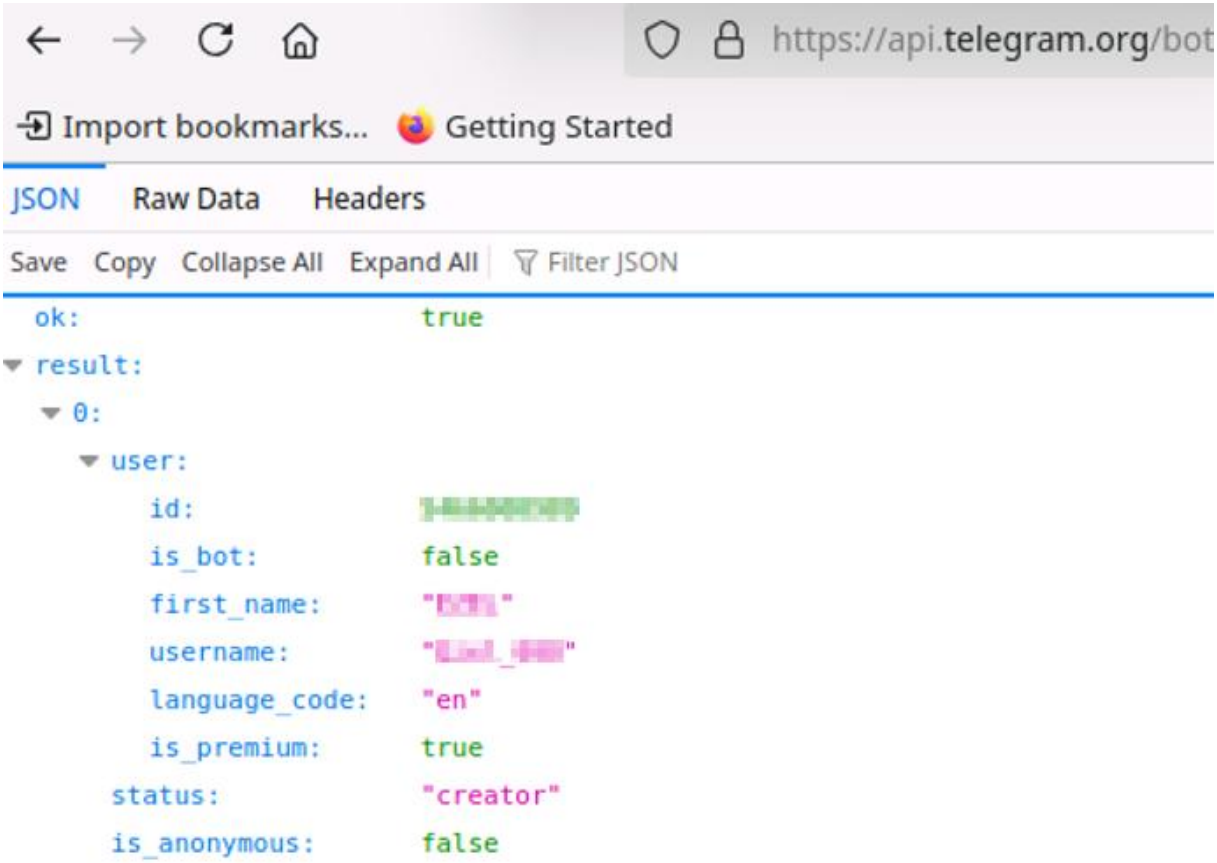
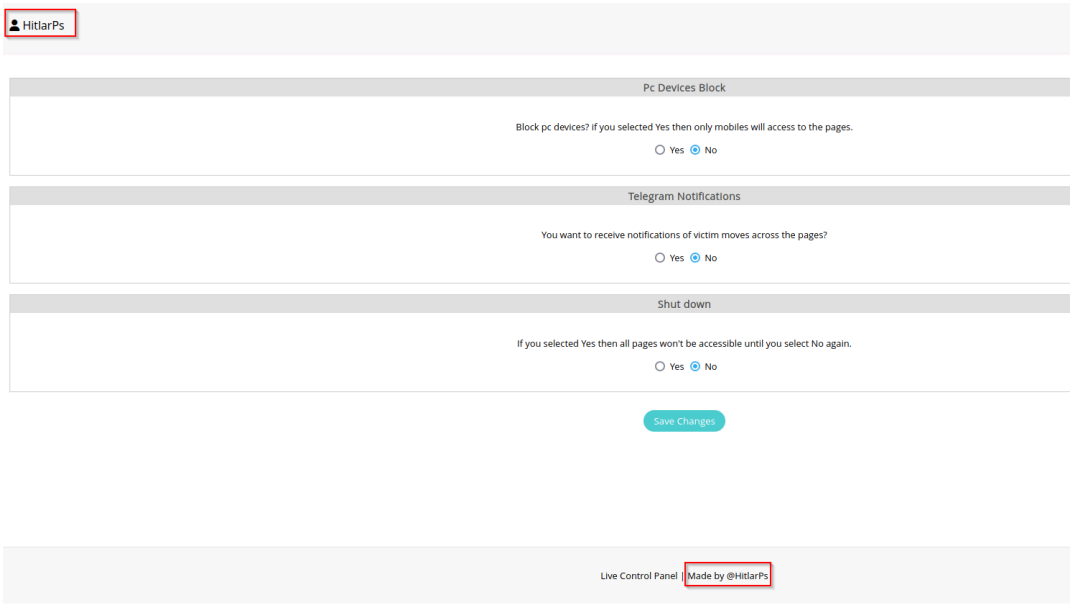


Figure 17: Recovering the username of the administrator of the Telegram bot connected to a phishing panel, using the Telegram API.

Additionally, on some panels, users have modified the username, which can be leveraged to find their account on Telegram. This is an evident OPSEC error, or a way for the threat actor to be known if it is his goal.



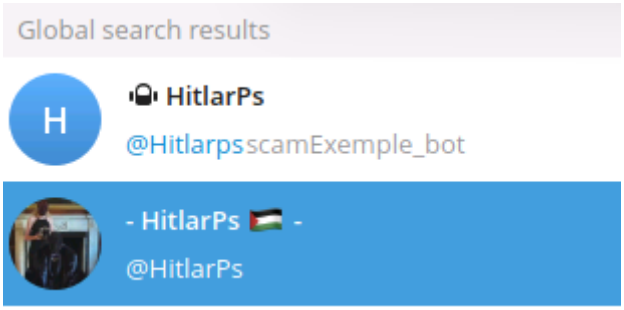


Figure 18: Finding a Telegram user leveraging the phishing toolkit, as evidence by his username.

Conclusion

Intrinsec CTI will continue to track this threat, potentially gaining information on the kit's author. We anticipate that threat actors will continue to use this toolkit for phishing purposes, usurping known companies. As seen in recent months, it is probable that more countries will be targeted by phishing domains associated with "Premium panel". As such, protecting against this threat is important and companies/institutions' defences as well as individuals should take proactive measures and good practices to stop credentials harvesting before it is too late.

III. Actionable content

1. Indicators of compromise

Value	Type	Description
kao.jfk.mybluehost.me/wp-admin/web/	URL	Qantas
laelenasa.com.ar/auqanta/web/	URL	Qantas
tly.vgj.mybluehost.me/cgi-bin/web/	URL	Qantas
zppwpailkq.cfolks.pl/ar/web/login.php	URL	Aruba
didc-malls.net/nk1/de/delogin/66f9272999098-70971.php	URL	SwissCom
redeem.quantasgift.store/v2/web/	URL	Qantas
gth.srl.mybluehost.me/wp-content/web/bill.php	URL	Air Canada
qantas.seawallet.pro/aufly/web/	URL	Qantas
cggelhs4fvad.adigeni.ge/eazy/web/	URL	EasyName
ryiucndes.mypi.co/T/il/index.php	URL	Israel Post
of-cyprusgroup.com/cy/auth/login.php	URL	Bank of Cyprus
profiles.riders.guide/js/web/	URL	Qantas
wordpress-983281-3799665.cloudwaysapps.com/wp-admin/ca/auth/entrar.php	URL	Crédit Agricole
0rc5zd5pdqbnlrkv5.adigeni.ge/eazy/web/	URL	EasyName
complete-card-tdn9g8zr3dqc.adigeni.ge/ccb/web/	URL	Card Complete
lna.ire.mybluehost.me/wp-content/web/	URL	Qantas
ezv.jnk.mybluehost.me/auth/login.php	URL	PostFinance
www.mobilvodafone.com/auth/auth.php	URL	Vodafone
authentication.watchsanda.com/auth/login.php	URL	EasyWeb
serwer2255313.home.pl/finan/finan/auth/login.php	URL	PostFinance
connect-client.serv00.net/app/app/login.php	URL	Netflix
snize-next.com/hy0/de/delogin/66e077efe7cf2-73438.php	URL	SwissCom
espace-documents-authsec-appmovil.codeanyapp.com/Particuliers/sg/web/wait.php	URL	Societe Generale
united-domains-gub9tvon.adigeni.ge/ud/web/add.php	URL	United Domains
webid.netcharge.lat/verif/miles-and-more-kreditkarte.com/web/login.php	URL	Miles & More
corres.live/GtTracking/auth/card.php	URL	Correos de Guatemala
atzqatavtz.adigeni.ge/wino/web/add.php	URL	SiteGround
tcuvbwgt8l.adigeni.ge/wino/web/add.php	URL	SiteGround
7f6n14eabe.adigeni.ge/wino/web/	URL	SiteGround

bbndf7evqc.adigeni.ge/wino/web/add.php	URL	SiteGround
qzif5odwmi.adigeni.ge/wino/web/add.php	URL	SiteGround
w4hquoo7dg.adigeni.ge/wino/web/add.php	URL	SiteGround
dervfpvcvy.adigeni.ge/ud/web/add.php	URL	United Domains
kamakatchi.serv00.net/NETFLIX/app/app/login.php	URL	Netflix
satfera.in/build/auth/	URL	Intuit
myj.pju.mybluehost.me/web/	URL	Qantas
clinicafatima.com/otp/auth/login.php	URL	OTP Bank
ltswedbank-ab.com/auth/login.php	URL	SwedBank
www.post-israel.savacrm.com/il/index.php	URL	Post Israel
ecomm-shop.org/kn21/page/wp/66c1c28a54602-47939.php	URL	Apple
dash-appserv.net/hg0/page/wp/66bd88d6bedde-23358.php	URL	Apple
urn.pyw.mybluehost.me/web/	URL	Qantas
pintacaritasmiami.com/.well-known/-/global/takare/login.php	URL	MBH Bank
casabeachfront.in/mainz/auth/entrar.php	URL	CaixaBank
domains.bavarian-marketing.org/wp//domains/clients/web/add.php	URL	Key-systems
lucassouzajlle.com/mains/auth/entrar.php	URL	CaixaBank
radiosouzahits.com.br/admin/swf/"/payment	URL	Qantas
swedbankgroup.info/auth/login.php	URL	SwedBank
onlineswedbank-lt.com/auth/login.php	URL	SwedBank
radionave.com/scripts/colorbox/images/ie6/'/payment	URL	Qantas
sparkteamsupport.com/web	URL	Spark New Zealand
swedbank-lt.online/auth/login.php	URL	SwedBank
acconnex.eu/app/login.php	URL	Orange
imprentacubodigital.com.ar/hu/auth/login.php	URL	Yettel
frezik-art.pl/finance/Financer/Pos/auth/login.php	URL	PostFinance
serwer2043802.home.pl//biblioteka2018/szablon/PostFinance/auth/login.php	URL	PostFinance
giermusicclub.com.ar/lt/auth/login.php	URL	SwedBank
stanfordheathaccountants.co.uk/cyprus/auth/login.php	URL	Bank of Cyprus
commerzbank-de-phototan.info/cmz.de/DE-commerzbanka_edit/DE-commerzbanka_edit/web/login.php	URL	Commerzbank
tfserviceupda.wpenginepowered.com/tf/de/home/login.php	URL	TF Bank

ebenezerbandeira.com.br/cgi-bin/web	URL	Qantas
ci45998.tw1.ru/caixa/home/entrar.php	URL	CaixaBank
campomaior.website.radio.br/imagens/ico_redes/web/payment	URL	Qantas
cidadejornal.website.radio.br/includes/web/payment	URL	Qantas
nerco.es/wp-includes/Text/Diff/Engine/host/auth/login.php	URL	CaixaBank
rockbyes.com/de/tf-bank/home/login.php	URL	TF Bank
radiothethemix.com/200/web/bill	URL	Qantas
app-update-service.site/wp-content/TF-0199/tf-banks/home/login.php	URL	TF Bank
heisateam.com/ar/servizo/home/loading1.php	URL	DPD
wise-idtransfer.napraw-agd.pl/valid/web/index.php	URL	Wise
wise-transfer.napraw-agd.pl/suift/web/index.php	URL	Wise
wise-signup.witchclean.com/web/index.php	URL	Wise
wise-line.nilangroup.com/lg/web/index.php	URL	Wise
centerpointaddisfurnishedapartment.com/yettel.hu/auth/login.php	URL	Yettel
wise-online.fabsmarketinggroup.com/sss/web/index.php	URL	Wise
targo-holiscarl1999281292.codeanyapp.com/identification-authentification/home/login.php	URL	Targo Bank
sb1.724.mytemp.website/s/auth/login.php	URL	PostFinance
transwise.nilangroup.com/verify/web/index.php	URL	Wise
tf-banks.online/De/tf-bank/home/login.php	URL	TF Bank
fpv.ths.mybluehost.me/SPK/Online/spa/home/bic.php	URL	Sparkasse
www.brilliantcctvcamera.com/spk/sparkasse%20de/spa/home/bic.php	URL	Sparkasse
ckx.cna.mybluehost.me/u.p.s/app/track.php	URL	UPS
kanonjdid.tempurl.host/xnallo/web/login.php	URL	Courier IT
of.cyprus.centerpointaddisfurnishedapartment.com/cyprus/auth/login.php	URL	Bank of Cyprus
highshopu.com/kWw3r/pos/auth/login.php	URL	CaixaBank
lizard.hu/sa/home/entrar.php	URL	STC Pay
a2.detaynet.com/SWISS/auth/login.php	URL	PostFinance
xqq.bof.mybluehost.me/mphb%202/2023/web/login.php	URL	TF Bank
xvb.zca.mybluehost.me/sp2/abonne/delogin/6641e4a0b0a76-99562.php	URL	Spotify
onlinegatewayunpaidfees.com/JFYRTADZ/index.php	URL	USPS
nilangroup.com/assets/online/web/index.php	URL	Wise

billsleek.in/re0/abonne/delogin/663cc2566f456-49777.php	URL	Spotify
xvb.zca.mybluehost.me/sp2/abonne/delogin/663cdc75b4f70-86660.php	URL	Spotify
dal4.hostclusters.com/~pwaprmaze/AKEMZLA/ZAMELZ/SG/web/login.php	URL	Societe Generale
reschedulepackonlineus.com/JFYRTADZ/index.php	URL	USPS
cyber_folks.schmerztherapie-schumann.de/c1s2e3rt5y6e-ndd/t-online_beta/web/user.php	URL	Cyberfolks
cyber_folks.kruzineser.org/c1s2e3rt5y6e-ndd/t-online_beta/web/user.php	URL	Cyberfolks
cyber_folks.scrimbus.de//c1s2e3rt5y6e-ndd/t-online_beta/web/user.php	URL	Cyberfolks
onlineuspsportalusa.com/JFYRTADZ/index.php	URL	USPS
drshamimkhan.in/config/sparkasse/spa/home/login.php	URL	Sparkasse
bakeforeme.corenetwork.net/mycouriers/web/	URL	Fastway Courriers
fordpussetto.com.ar/sparkassea/sparkasse/spa/home/bic.php	URL	Sparkasse
sidikhsu.com/sparkasse/spa/home/bic.php	URL	Sparkasse
wiseonline.aykernasbungalov.com/wises/web/index.php	URL	Wise
receber-post-correios-rrfd.codeanyapp.com/SG1/sg/web/login.php	URL	Societe Generale
www.southerntennis.com/~pamrlr/PP/sg/web/login.php	URL	Societe Generale
dolphin4k.com/jw/wises/web/index.php	URL	Wise
musclemeal.co.in/mll/comp/de/	URL	Apple
web-seb.com/web/login.php	URL	SEB Bank
69c.6b5.mywebsitetransfer.com/SWISS/auth/login.php	URL	PostFinance
postfnc-contact.de.swtest.ru/de/secure/auth/login.php	URL	PostFinance
internetbanking.ne-tu.eu//libra-ro/mm/web/login.php	URL	Libra Internet Bank
bar.bgd.mybluehost.me/idr/DEsparkasse/spa/home/login.php	URL	Sparkasse
swissonlinecom.com/fa/99/web/login.php	URL	SwissCom
eti.hgn.mybluehost.me/wp-admin/css/auth/home/login.php	URL	Sparkasse

/sparkasse-login-secured-sparkasse.codeanyapp.com/sparkasse/css/auth/home/login.php	URL	Sparkasse
wordpress-168935-0.cloudclusters.net/spa/spa/hom/spar/spa/home/bic.php	URL	Sparkasse
www.moraesconcreto.com/wp-admin/nordddea/auth/login.php	URL	Nordea Bank
l75.eee.mywebsitetransfer.com/Norde-a/auth/login.php	URL	Nordea Bank
themarketersdream.com.au/auth/login.php	URL	Bank of Cyprus
hostnow.co.ke/twentytwent/auth/home/login.php	URL	Sparkasse
serwer2397890.home.pl/imodzeb/PostFinance/Finance/auth/login.php	URL	PostFinance
ashadeofjade.com/sar/home/tarjeta.php	URL	SaudiPost
www.hospitalcovadonga.com/wp-content/languages/themes/finance/auth/login.php	URL	PostFinance
myblog-on8u3ksh23.live-website.com/wp-admin/A/spa/home/login.php	URL	Sparkasse
www.postbank.fameseminuevos.com/app/loginos.php	URL	PostBank
dzempas.com/wp-amln.php/auth/login.php	URL	Bank of Cyprus
littlelight-baby.com/vod/auth/login.php	URL	Vodafone
signin-postfinanceaccount-ch.sslawoff.com/id/auth/login.php	URL	PostFinance
fastupdate.tempurl.host/vubs/vubs/web/login.php	URL	Vub Banka
politicsniger.com.ng/wp-content/upgrade/auth/login.php	URL	PostFinance
obzoronlinecasino.ru/wp-admin/stand/app/logins.php	URL	Standard Bank
sparrow.de/sa/home/tarjeta.php	URL	STC Pay
www.edenthub.com/Downloads/consor/web/login.php	URL	BNP Paribas
rfpiliberia.com/Application/DE/consor/web/login.php	URL	BNP Paribas
thetrend.blog/wp-admin/search/web/login.php	URL	TF Bank
www.turismotierraestella.com/fonts/_notes/tf/web/login.php	URL	TF Bank
vfo.hdv.mybluehost.me/website_e9e0f586/A/tfsf/2023/web/login.php	URL	TF Bank
postsendungschweiz.sviluppo.host/paket/global/index.php	URL	SwissPost

teamglobal-info1online.codeanyapp.com/SPK/Sparkass/auth/home/login.php	URL	Sparkasse
clinicaperezdelolmo.com/wp-includes/assets/75982135469720125 5/auth/651f0b7cc227dcfa4c39a30c159dabf5.php	URL	CaixaBank
serwer1739297.home.pl/-/blog/fio/fiobanka/auth/login.php	URL	Fio Banka
tareeqalghaith.com/bas2024/auth/f8bc37e4d02386531effa2f0382cf809.php	URL	CaixaBank
cd69506.tw1.ru/PostFinance/auth/login.php	URL	PostFinance
cznew.tempurl.host/aji/cz/web/login.ph	URL	Fio Banka
abelza.pl/cy/auth/login.php	URL	Bank of Cyprus
everdaysca.temp.swtest.ru/up/spaaa/sparkasse/spa/home/login.php	URL	Sparkasse
melon-soft-hosting.com/cy/auth/login.php	URL	Bank of Cyprus
support-contact-hmz2.codeanyapp.com/D/Sparkass/auth/home/login.php	URL	Sparkasse
bol.yqp.mybluehost.me/css/auth/home/login.php	URL	Sparkasse
vdv6y.live/D/Spvrkvss/auth/home/login.php	URL	Sparkasse
universal-ferretera.com/mvm/auth/login.php	URL	MVM
glenorchyinfocentre.co.nz/.well/3568653000/spa/home/login.php	URL	Sparkasse
swed.lietuva.conextium.com/auth/login.php	URL	SwedBank
rainlapo.com/wp-content/twentytwentyone/auth/home/login.php	URL	Sparkasse
hpp.b7b.mywebsitetransfer.com/SWISSPASS/auth/login.php	URL	Schweizerische Bundesbahnen
resultados.santaanadedios.com/css/auth/home/login.php	URL	Sparkasse
trocken.online/twentytwentyone/auth/home/login.php	URL	Sparkasse
admin-paroisses42.fr/glpi/vendor/htmlawed/htmlawed/sparkasse/auth/home/login.php	URL	Sparkasse
emswidebay.com.au/rel/res/home/entrar.php	URL	Alrajhi Bank
tadbircard.ir/govsa/res/home/tarjeta.php	URL	Ministry of Human Ressources
bomnegociorural.com.br/d/home/entrar.php	URL	Central Bank of Saudi Arabia
fio.cz.k1informatica.com.br/auth/login.php	URL	Fio Banka
www.fio.cz.yviitv.com/auth/login.php	URL	Fio Banka
musclemeal.co.in/fonts/fb0/akkount/de/index.php	URL	Swisscom

bubblecard.org/bubblecard.lk/KJ0/akkount/de/index.php	URL	Swisscom
lt-coach.com/wp-content/plugins/css/akkount/de/index.php	URL	Swisscom
capetownew.tempurl.host/wp-tach/cz/web/login.php	URL	Fio Banka
rootland.in/mo0/akkount/de/index.php	URL	Swisscom
rootland.in/wp-includes/Requests/bv1/akkount/de/index.php	URL	Swisscom
millenium-velegozh.ru/news/files/cz/web/login.php	URL	Fio Banka
otpbank.cs-group.digital/post/auth/login.php	URL	OTP Bank
cec.ro.fabricebernasconiborzi.com/auth/login.php	URL	CEC Bank
lumdevelopmentresearch.com/wp-content/plugins/auth/login.php	URL	PostFinance
anaika.birlanavya63a.com/wp-includes/Requests/Cookie/auth/login.php	URL	PostFinance
fort-client.college/consor/web/login.php	URL	BNP Paribas
id-kontoaktualisieren383266.codeanyapp.com/tr/home/login.php	URL	Targo Bank
www.ljrtrucking.com/Configs/PostFinance/auth/login.php	URL	PostFinance
decorfine.com.ec//.well-known/pki-validation/login/	URL	Alpha Bank
posttfiinancelusi.com/PostF/auth/login.php	URL	PostFinance
www.postfinance.ch/ap/ba/ob/html/finance/home?login	URL	PostFinance
shrioswalsamaj.com/wp-content/plugins/eqlfrvxfrz/ve/web/login.php	URL	TF Bank
aktualisierung-kontoinformationen-marklisy1992160133.codeanyapp.com/ag/home/login.php	URL	Targo Bank
occasionifissowindtre.com/auth/login	URL	CEC Bank
otpdirekt.ro.pitruzzellaimpianti.it/auth/login.php	URL	OTP Bank
otpdirekt.sytes.net/otp/auth/login.php	URL	OTP Bank
www.santander-kreditkort-consumer.grey.com.pk/.f6f1fcaf81183bea5949c9ef837912945/	URL	Santander
kundenservice-ingdirekt-girokonto-appmovil.codeanyapp.com/FR/sg/web/login.php	URL	Societe Generale
secure3-mabanque-bnpparibas.fr/auth/login.php	URL	BNP Paribas
smartbank-otpbank.nobokoli.com/auth/login.php	URL	OTP Bank
arrarra.sa.com/app/login.php	URL	Netflix

suryamatrimony.in/.f6f1fcaf81183bea5949c9ef837912945/	URL	Santander
www.smartbank-otpbank.pieseimp.ro/auth/login.php	URL	OTP Bank
atchondabikestore.com/wp-admin/maint/web/login.php	URL	TF Bank
48j.e35.mywebsitetransfer.com/carrefoures/auth/login.php	URL	Carrefour
areabienesyservicios.com/res/res/home/entrar.php	URL	Ministry of Human Ressources
whitefoxpouch.com/a/advancia/sparkasse/spa/home/bic.php	URL	Sparkasse
bundesanzeiger.gb-clinic.com/.f6f1fcaf81183bea5949c9ef837912945/	URL	Santander
fomrationa.temp.swtest.ru/kada/spaaa/sparkasse/spa/home/login.php	URL	Sparkasse
regular-dane.10web.site/de/mphb/2023/web/login.php	URL	TF Bank
billsleek.in/ic0/comp/de/	URL	Apple
billsleek.in/ip0/de/akk/index.php	URL	SwissPost
group-ibannk.web12010.web09.bero-webspace.de/api/auth/login.php	URL	NBG
myblog-mf8zji6ax8.live-website.com/mphb/2023/web/login.php	URL	TF Bank
www.conectandocontumagia.com/lifrong/home/index.php	URL	SwissPost
ibnk-gr-info.web12010.web09.bero-webspace.de/api/auth/login.php	URL	NBG
secure16-bnpparibas.fr/auth/login.php	URL	BNP Paribas
ctbc-tw.icepluschap.com/tw/ctbcbank_panel/auth/login.php	URL	CTBC Bank
secure19-bnpparibas.fr/auth/login.php	URL	BNP Paribas
secure8-bnpparibas.fr/auth/login.php	URL	BNP Paribas
servicecarfourassist.organiccrap.com/V0reER/index.php	URL	Carrefour
srv204523.hoster-test.ru/b456rt46d/4bre41gd2/xc4v21eczr/web/Login.php	URL	VUB Banka
vub.companyonlinecom.site/vub/web/login.php	URL	VUB Banka
automotive5.sa.com/login/app/login.php	URL	Netflix
secure213.inmotionhosting.com/~cocoam6/wp-includes/js/tinymce/plugins/compat3x/css/libra/web/login.php	URL	Libra Internet Bank

nuevolead.com/tflogist/web/login.php	URL	TF Bank
medra.sa.com/login/app/login.php	URL	Netflix
secure17-bnpparibas.fr/auth/login.php	URL	BNP Paribas
ccmmmm.sa.com/login/app/login.php	URL	Netflix
www.indasiaglobal.com/-/webd/c/h/blue/11/23/2.99/d/e/8z52zee520ee/x854z1z5ze0000e/Sw/de/index.php	URL	SwissPost
ergstaffingtemps.com/wp-admin/SAOPAZZE/home/card.php	URL	Targo Bank
statelinks.net/rmb/cxv/auth/login.php	URL	First National Bank
www.nd-more-kartenabrechnung.de/il/index.php	URL	Israel Post
buy.bigbenespana.es/cgi-biin/home/entrar.php	URL	CaixaBank
tourised.com/postbankgirokonto24/post1/423565/2455/de/user.php	URL	PostBank
toursgaudi.com/zahlung/home/index.php	URL	SwissPost
billsleek.in/cd1/akkount/de/index.php	URL	SwissCom
billsleek.in/ar0/st/arr/login.php	URL	Aruba
bnkgroup-gr.dorian.hostline.net.pl/api/auth/login.php	URL	NBG
iaiqh.ac.id/auth/login.php	URL	NBG
inndesage.org/mrd/fnbvics/mp33rd/auth/login.php	URL	First National Bank
shrey.prep.co.in/auth/login.php	URL	NBG
www.nbg.group.paymentsclaim.com/auth/login.php	URL	NBG
afiliados.emanuelhallef.com.br/appcha/home/entrar.php	URL	CaixaBank
atualoja.com/zahlung/home/index.php	URL	SwissPost
lasaath.com/Postfinance/home/login.php	URL	SwissPost
organizacionvip.com/zahlung/home/index.php	URL	SwissPost
tfservv-abdofreedy27329072.codeanyapp.com/mphb/2023/web/login.php	URL	TF Bank
icaroaph.com/liefere/home/index.php	URL	SwissPost
cristianheredia.com/home/index.php	URL	SwissPost
secure257.inmotionhosting.com/~dralsafadi/inro/web/login.php	URL	ING
mivcard.com/vieca/home/index.php	URL	SwissPost
chcfngo.in/de/mphb/2023/web/login.php	URL	TF Bank
mail.mindmateapp.com/error/israel2k23/il/step2.php	URL	Israel Post
auth.facture-comptable-enligne.xyz/auth/login.php	URL	Miles & More
dsfp5.ru.com/login/app/login.php	URL	Netflix
jsdmadeira.pt/home/index.php	URL	SwissPost
https://israelbepostcoil.it/il/index.php	URL	Israel Post

simasbos.id/assets/font/IKUJYHTGFR/2023/web/login.php	URL	TF Bank
nenaotransportes.srv.br/vieca/home/index.php	URL	SwissPost
gertfb.tempurl.host/look/web/login.php	URL	TF Bank
anunciosparaempresas.com.br/wp-content/upgrade/tf/web/login.php	URL	TF Bank
digistore.myanmarcafe.trade/vieca/home/index.php	URL	SwissPost
hamam-wellness.com/spa/home/card.php	URL	Sparkasse
opdatter-informasjon.dynv6.net/.f6f1fcaf81183bea5949c9ef837912945/	URL	Santander
sfr-annulation-esim.fr/fr/51043913074cd820fe0fdafa16e77b07.php	URL	SFR
alpha.parcelvit.com/login/	URL	Alpha Bank
brookfieldagricultural.com.au/wp-admin/yuoi/home/card.php	URL	Targo Bank
doutshstg.wpenginepowered.com/al/home/login.php	URL	TF Bank
salviano.udoit.com.br/home/index.php	URL	SwissPost
teamafitness.com/wp-admin/ibola/home/card.php	URL	Targo Bank
www.seoppcnews.com/wp-admin/Sapoer/home/card.php	URL	TF Bank
www.mediamondo.com/vieca/-/home/index.php	URL	SwissPost
ctbcbank-com-taseneh779753577.codeanyapp.com/cbtc/src/login.php	URL	CTBC Bank
smart.patrickattema.nl/home/index.php	URL	SwissPost
service-annulation-sfr.fr/fr/login.php	URL	SFR
annulation-e-sim-sfr.fr/fr/login.php	URL	SFR
ghi.billsleek.in/fg1/akkount/de/index.php	URL	Schweizerische Bundesbahnen
app.follieeventi.it/i/c/auth/login.php	URL	CEC Bank
www.tryyourweb.com/post/home/index.php	URL	SwissPost
app.fnaemiliaromagna.it/ign/cec/auth/login.php	URL	CEC Bank
service-sim-sfr.fr/fr/login.php	URL	SFR
ing.login-nic-ae.com/ign/gr/auth/login.php	URL	NBG
oppdatterkontanktinformasjonn.de/.f6f1fcaf81183bea5949c9ef837912945/	URL	Santander
tw-post-safiramira099303091.codeanyapp.com/web/login.php	URL	TF Bank
meine-tfbank-de-taseneh779753577.codeanyapp.com/web/login.php	URL	TF Bank
billsleek.in/sb3/akkount/de/index.php	URL	Schweizerische Bundesbahnen

app-153bc257-0381-4ee7-ba06-16f8e40914fc.cleverapps.io/tar/home/login.php	URL	Targo Bank
boxer.vivawebhost.com/~sharcoho/udomasa/vendor/brick/math/src/Internal/Calculator/inro/web/login.php	URL	ING
secure253.inmotionhosting.com/~belkoc5/wp-includes/js/tinymce/plugins/compat3x/css/inro/web/login.php	URL	ING
delivery-club-jacobs-millicano-test.digital-preprod.ru/dpo/home/index.php	URL	SwissPost
dev-s-id-check.pantheonsite.io/spa/home/card.php	URL	Sparkasse
licenselinks.com/vieca/home/index.php?	URL	SwissPost
secure4-bnpparibas.fr/auth/login.php	URL	BNP Paribas
ausfilliing.duckdns.org/Au/global/index.php	URL	Australian GOV
zahlen-diepost.com/global/index.php	URL	SwissPost
srv199153.hoster-test.ru/n4f6g54h6r5t/b489t4h3f2/web/login.php	URL	Host Europe
swiss-post-ch.com/global/index.php	URL	SwissPost
musclemeal.co.in/sp06/akkount/de/index.php	URL	SwissCom
secure2-credit-agricole.fr/fr/login.php	URL	SFR
divinepublicschool.in/ax04/ax/axa-meine/index.php	URL	AXA
secure3-sfr.fr/fr/login.php	URL	SFR
diepost-login.com/global/index.php	URL	SwissPost
article.wefre.nl/vieca/home/index.php	URL	SwissPost
www.npt-chain.com/vieca/home/index.php	URL	SwissPost
spl-service-sa.com/en/bill.php	URL	SPL Post
usps.business/global/index.php	URL	USPS
postal-service.co/ch//de/index.php	URL	SwissPost
www.dhf-hilden.de/romavbv/web/login.php	URL	UniCredit
musclemeal.co.in/ck1/akkount/de/index.php	URL	SwissCom
www.instelatorim10.co.il/-/home/index.php	URL	SwissPost
depkhongtuoi.com/ch-liefrung/home/index.php	URL	SwissPost
taxibinhduong247.net/wp-content/languages/seicea/home/index.php	URL	SwissPost
purehoneyonline.com/kon/akkount/de/index.php	URL	SwissCom
muscleforce.in/jprones/akkount/de/index.php	URL	SwissCom
sonu.billsleek.in/jqGrid/frk/meine/IDPSTVONSA/index.php	URL	SwissPost
cindyfernandezstudio.com/vieca/home/index.php	URL	SwissPost
postbankmeinbestsign24h.elevadoresvision.com.br/postde1/423255/de/64AFD9050FBB1.php	URL	Postbank

purehoneyonline.com/ftx/st-point/clients/login.php	URL	ING
guciabu.com/pt/app/login.php	URL	Netflix
n2meinpost24h.elevadoresvision.com.br/postde1/324553/de/64A530E2B872B.php	URL	Postbank
die-osteopathin-in-wien.at/lvepayd/home/index.php	URL	SwissPost
activation-cle-digitale-bnp-paribas.fr/auth/login.php	URL	BNP Paribas
blastdesal.com/seices/home/index.php	URL	SwissPost
hotelcampestrelafloresta.com/-/seices/home/index.php	URL	SwissPost
myalpha-gr24.cursosglaucoleyser.com.br/alpha1/324344/2344/gr/login.php	URL	Alpha Bank
ml-santanderesbanco24h.paisrecords.com/Qyh9C9b2YDX6g4n/santander24h/X46b9DngQ9Yy2Ch/es/login.php	URL	Santander
todayuupdates.tempurl.host/tmb/tf/tf/web/login.php	URL	TF Bank
uwtestserver3.nl/home/index.php	URL	SwissPost
www.postbankdebest24h.biocroche.com.br/bestsignpostde24h/733dAT6jLAw8fb/b6fd38w37jTALA/de/user.php	URL	Postbank
bnpparibas-authentification.fr/auth/login.php	URL	BNP Paribas
postbankde24hbestsigne.robotclub.com.br/meinbestsigne24/jAwT7b3f6L3dA8/7jAfAdTb63Lw38/de/user.php	URL	Postbank
postbankmeinbestsign24h.elevadoresvision.com.br/post1/423545/de/648B0A104BD95.php	URL	Postbank
activation-cledigitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
bnpparibas-activation-cle-digitale.fr/auth/login.php	URL	BNP Paribas
postbank1bestsignwinde1.connectplus.co.mz/post1/244543/4314/de/6486DF4479403.php	URL	Postbank
bnpparibas-nouvelle-cle-digital.fr/auth/login.php	URL	BNP Paribas
nouveau-service-bnpparibas.fr/auth/login.php	URL	BNP Paribas
nouvelle-cle-digitale-bnp-paribas.fr/auth/login.php	URL	BNP Paribas
nouvelle-cle-digitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
andlpostbankbestsigne24h.despachantersantos.com.br/post1/234544/1377/de/6480653EEC279.php	URL	Postbank
meinpostbankdebest24h.despachantersantos.com.br/post1/453443/4227/de/6480650BDD441.php	URL	Postbank
pixelinegroup.com/postde1/203943/2433/de/648036F7977D8.php	URL	Postbank
service-clients-sfr.fr/fr/login.php	URL	SFR
bnp-paribas-service-clients.fr/auth/login.php	URL	BNP Paribas

nosservice-bnpparibas.fr/auth/login.php	URL	BNP Paribas
die-post.co/ch/de/index.php	URL	SwissPost
service-clients-bnp-paribas.fr/auth/login.php	URL	BNP Paribas
pixelinegroup.com/postde1/203943/2433/de/647EFFE0977E0.php	URL	Postbank
postbankdebestsigne24h.rsantosseguros.com.br/TA3jd7AwfbL638/TA3jd7AwfbL638/de/647F00642B3E2.php	URL	Postbank
postbankdeibest24h.despachantersantos.com.br/post1/245344/3245/de/647F4CEA3686E.php	URL	Postbank
demande-esim-sfr.fr/fr/login.php	URL	SFR
sfr-demande-e-sim.fr/fr/login.php	URL	SFR
conversoresycables.com/pb/de/647DB5B0917DB.php	URL	Postbank
m2einpost2457.vicsis.com.br/postde1/245478/de/647DDCC1D96E0.php	URL	Postbank
www.postbankdebest24h.biocroche.com.br/postde24h/ATfj33b7dLwA68/6AwLd7b338jfTA/de/user.php	URL	Postbank
service-mabanque-bnpparibas.fr/auth/login.php	URL	BNP Paribas
accerpostfinarce.photoracertv.app/clientes24h/yZ4He8wcWQ764a/home/login.php	URL	PostFinance
bnpparibas-service-client.fr/auth/login.php	URL	BNP Paribas
kaya-group.eu/wp-content/plugins/akismet/views/sviezas/home/index.php	URL	SwissPost
valuecart.in/postch1/327892/3799/home/login.php	URL	PostFinance
varshawires.com/postch2/378292/7622/home/login.php	URL	PostFinance
nos-clients-bnpparibas.fr/auth/login.php	URL	BNP Paribas
bnpparibas-nos-clients.fr/auth/login.php	URL	BNP Paribas
kombbansrestaurant.com/post1/237888/0488/de/user.php	URL	Postbank
royalserenity.in/post1/829302/3722/de/user.php	URL	Postbank
unitechme.com/post1/328903/2987/de/user.php	URL	Postbank
rengelinkfonds.nl/shppment/home/index.php	URL	SwissPost
rhscranes.com/depost2/289819/2811/de/user.php	URL	Postbank
shivaconstructions.co/post1/328901/3211/de/user.php	URL	Postbank
todayuupdates.tempurl.host/nikmk/tf/tf/web/login.php	URL	TF Bank
www.monterreydelsur.com/post1/329021/3800/de/user.php	URL	Postbank
bankingpostbansign23.partywebshop.com/H2rp32R4eFnk5N/de/user.php	URL	Postbank

melnpostdesumzug.dtmteam.com/enpH42325FkrRN/de/user.php	URL	Postbank
comerzbanc.tel/lp/login/web/login.php	URL	Commerzbank
rawqha.com/commerzbank.de/web/login.php	URL	Commerzbank
www.commerzbank-login-up.multifilium.com/web/login.php	URL	Commerzbank
kunden.commerzservice.eu/web/login.php	URL	Commerzbank
grupopercon.com/wp-content/cai/home/entrar.php	URL	CaixaBank
caixadirectaonline.cgd-pt.tel/cdo/login.php	URL	Caixa Geral de Depósitos
assistance-swiss-post.info/de/index.php	URL	SwissPost
miseajour-cledigitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
votre-cledigitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
sim-sfr-service.fr/fr/login.php	URL	SFR
cle-digitale-service-bnpparibas.fr/auth/login.php	URL	BNP Paribas
bnp-paribas-nouvelle-cle-digitale.fr/auth/login.php	URL	BNP Paribas
bnpparibas-nouvelle-cle-digitale.fr/auth/login.php	URL	BNP Paribas
bnp-paribas-service-cle-digitale.fr/auth/login.php	URL	BNP Paribas
votre-nouvelle-cle-digitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
votre-nouvelle-cledigitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
service-cledigitale-bnp-paribas.fr/auth/login.php	URL	BNP Paribas
nouvelle-cledigitale-bnpparibas.fr/auth/login.php	URL	BNP Paribas
sienahandmadeleatherbags.com/homr/hom/app/login.php	URL	Netflix
bnpparibas-service-cledigital.fr/auth/login.php	URL	BNP Paribas
karacarulo.com.tr/menu/43356NT/app/login.php	URL	Netflix
renovvi.futuraproduction.it/servizipagamento/web/login.php	URL	Aruba
servizi.futurapress.it/servizipagamento/web/login.php	URL	Aruba
www.bankajk.com/rennovi/web/login.php	URL	Aruba
arubahosting.futurapress.it/file/servicehomeit/web/login.php	URL	Aruba
delinquenttaxsales.com/5235v/app/login.php	URL	Netflix
cia.4moor.it/avvizo/rennnove/web/login.php	URL	Aruba
track-posta-romana.com/post/confirm.php	URL	Posta Romana
dik.lelicriso.it/avvizo/rennnove/web/login.php	URL	Aruba
applepay-mena.com/id/confirm.php	URL	Apple
aza.scia-a-roma.it/conferma/web/login.php	URL	Aruba
des.fabbroh24roma.it/conferma/web/login.php	URL	Aruba
ele.sos-elettricistaroma.it/conferma/web/login.php	URL	Aruba

server.bertuzzitravel.com/conferma/web/login.php	URL	Aruba
apu.impresapuliziediamante.it/rennovi/web/login.php	URL	Aruba
dep.autospurgoh24firenze.it/rennovi/web/login.php	URL	Aruba
www.jobsindubai.com/sendgrid/N548789564/app/login.php	URL	USPS
perfectway.me/wp-content/plugins/ioptimization/cuenta/home/entrar.php	URL	CaixaBank
www.logiroad.ci/wp-content/plugins/apikey/validar/home/entrar.php	URL	CaixaBank
getnew.in/admin/controller/extension/extension/app/home/entrar.php	URL	CaixaBank
sportsmansharbor.net/tickets/DE548792164/de/	URL	Deutsche Post
santander-service.com/app/login.php	URL	Santander
www.support-access.cf/app/login.php	URL	Netflix
www.support-access.peachmusicla.com/app/login.php	URL	Netflix
www.bottegafacile.it/modules/mod_simplefileuploadv1.3/elements/S654F65S448S7F87G8/home/entrar.php	URL	CaixaBank
aspirebuildanddesign.com/SA654D94Z6Z4D6/home/entrar.php	URL	CaixaBank
yurimagoori.com/Z87D94Z64R96EZ546E/home/entrar.php	URL	CaixaBank
faporbaz.com/wp-content/plugins/fecclfkawd/65S46A549846R56/home/entrar.php	URL	CaixaBank
adestrarseupet.com.br/wp-content/plugins/biakvnctnl/Q654AD46546546T546R546R/home/entrar.php	URL	CaixaBank
bellydiet.com.br/A5D8D8T7Y8RE8/home/entrar.php	URL	CaixaBank
elbe.co.jp/news/wp-content/plugins/dzjoskqgvj/5S46F56G5G4/home/entrar.php	URL	CaixaBank
bnpparibasconnexion.fr/app/id.php	URL	BNP Paribas
cloud.physik-patio13.de/validar/home/entrar.php	URL	CaixaBank
kaqcnadqbo.cfolks.pl/65A6498R46T546/home/entrar.php	URL	CaixaBank
req-cap01w.net/auth/signin.php	URL	Capital One
pycwckviqz.cfolks.pl/654654R4TY44Y/home/entrar.php	URL	CaixaBank
www.watch-support.cf/app/login.php	URL	Netflix

www.watch-support.starpizzapakistan.com/app/login.php	URL	Netflix
www.watch-support.ml/app/login.php	URL	Netflix
www.dessertstory.co/depost/de/	URL	Deutsche Post
www.netflix-esupport.ml/app/login.php	URL	Netflix
www.qatarpost.shatta.net/ar/	URL	Qatar Post
parturier-avocats.fr/wp-content/plugins/alpha/login/	URL	Alpha Bank

2. Recommendations

To defend against this threat, Intrinsec CTI recommends:

- Install CanaryTokens on your public facing websites and pages used by clients. If a content is copied directly from the pages where a token is installed, it will create an alert.
- Block the IOCs provided in the Indicators of compromise section of this analysis. You can also subscribe to a CTI feed to continuously obtain fresh IOCs associated with this threat (and other threats).
- Monitor the creation of domain names spoofing your brand and demand their takedown.
- Train your employees to recognise phishing methods and always verify if a domain is legitimate before entering their credentials, and not open links sent by phishing emails.