SPM55: Ascending the Ranks of Indonesian Phishing As A Service Offerings

domaintools.com/resources/blog/spm55-ascending-the-ranks-of-indonesian-phishing-as-a-service-offerings

DOMAINTOOLS
SPM55: ASCENDING THE RANKS OF INDONESIAN PHISHING AS A SERVICE OFFERINGS

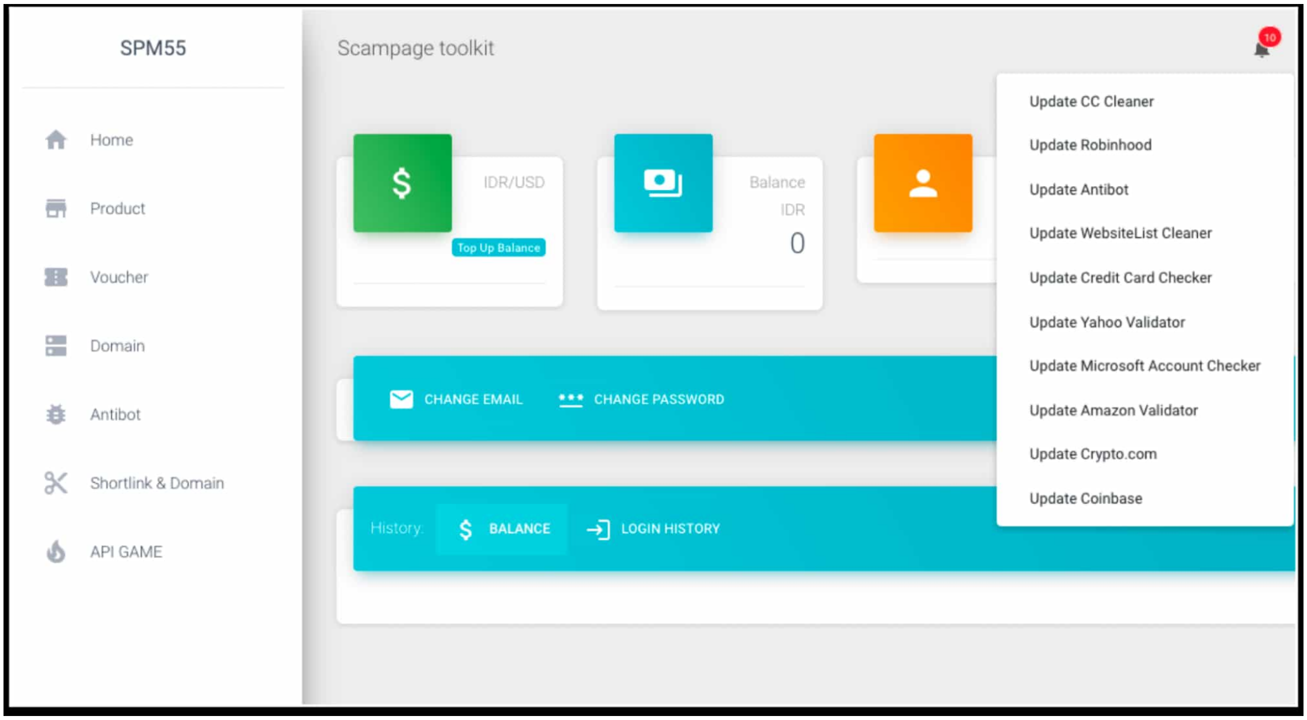
Who is SPM55?

Although SPM55 is a relative newcomer to the Indonesian cybercrime community, a marked uptick in activity and known customers over the last several months suggests this group seeks to scale their business operation, possibly in response to the collapse of competing Indonesia-based phishing vendors.

SPM55 offerings target a number of popular services, technology companies, and financial institutions. Some examples include Coinbase, Netflix, Amazon, and Ebay. Another noteworthy characteristic of SPM55 is their willingness to pivot rapidly based on customer feedback and expand their customer base by releasing new phishing kits quickly. Further, SPM55 offers *a la carte* credit card checkers and account validators which are frequently used for phished credential and payment data validation. Another add-on is an “antibot” service which SPM55 resells. In this context, such service reduces automated detection rates and thwarts security vendors by identifying and redirecting sessions to innocuous websites if a session appears to be inauthentic–that is, a session not belonging to a valid phishing target.

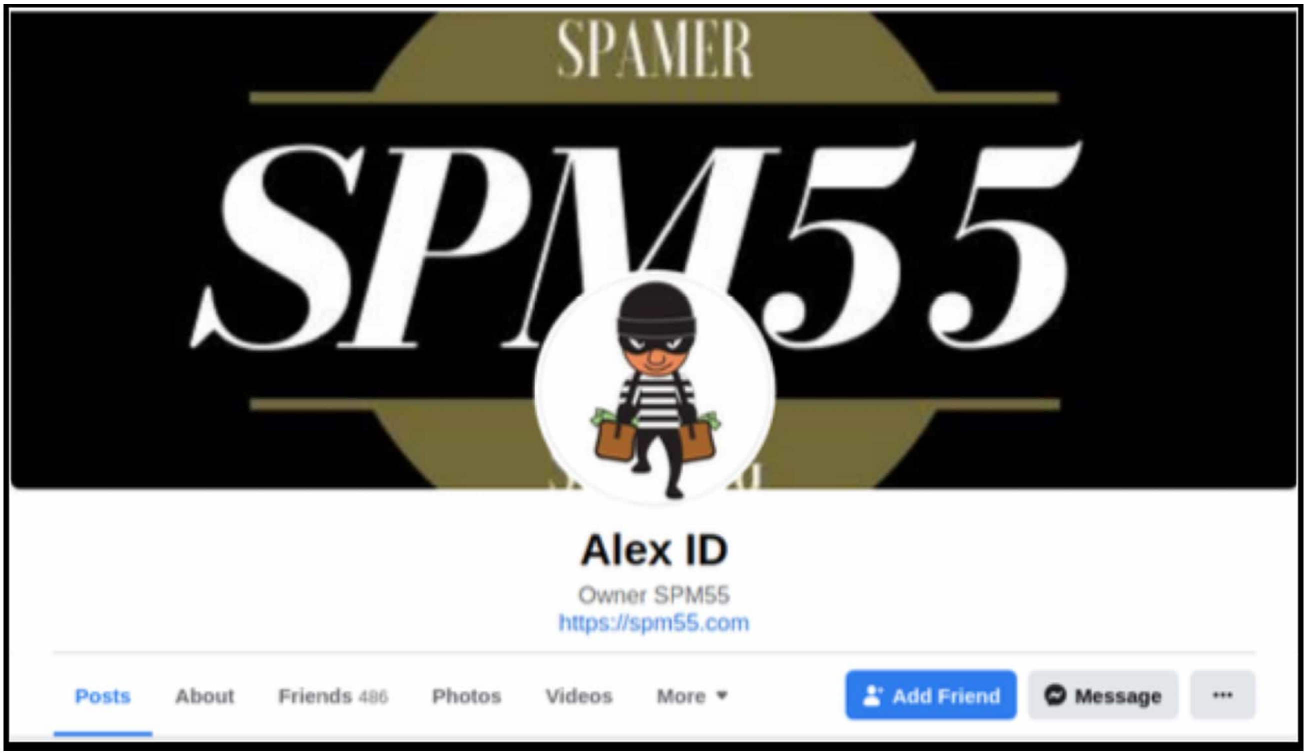
SPM55 phishing pages and custom lures appear to focus on the typical "your account is disabled" types of phishing page, and support not only fields for account credentials, but also what is commonly known in cybercrime communities as "fullz" or "full personal information" which can be used to commit several types of fraud.

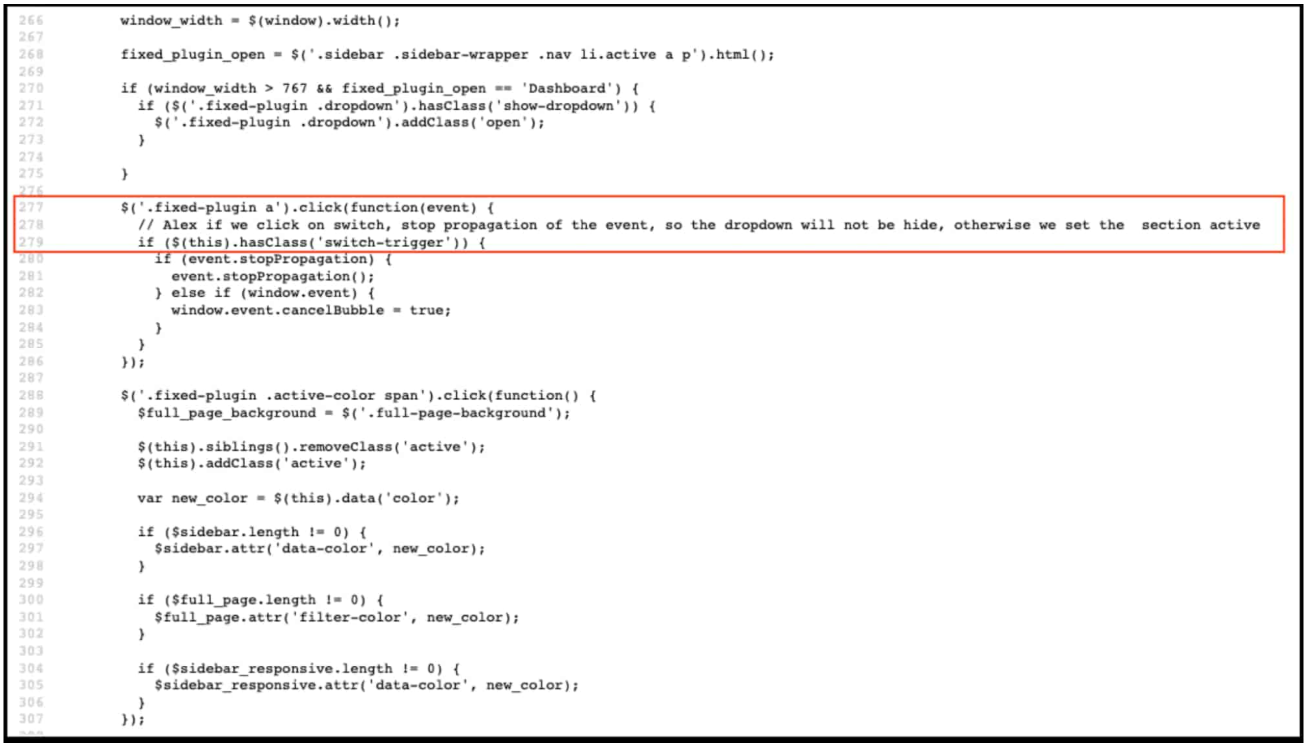
Written in PHP and bearing a strong resemblance to–and at times outright copying–those offered by cracked versions of 16Shop and Young Sister, SPM55's phishing kits and management panel are of above-average quality and have higher than average success rates compared to other phishing kits. Based on customer preference, deployed and properly licensed phishing kits send victim data to operators via email or Telegram. Notably, credential processing appears to send victim information to a SPM55-controlled management server as well, likely providing SPM55 with copies of the credentials stolen by their customers. Siphoned data is likely sold or used for fraudulent purposes by SPM55 administrators. In short, SPM55 may scam their own customers. Because stolen credentials and personal information are also likely siphoned to SPM55 administrators, the risk of harm from such phishing activity at the hands of a competent cybercriminal is likely to be severe.



Behind SPM55

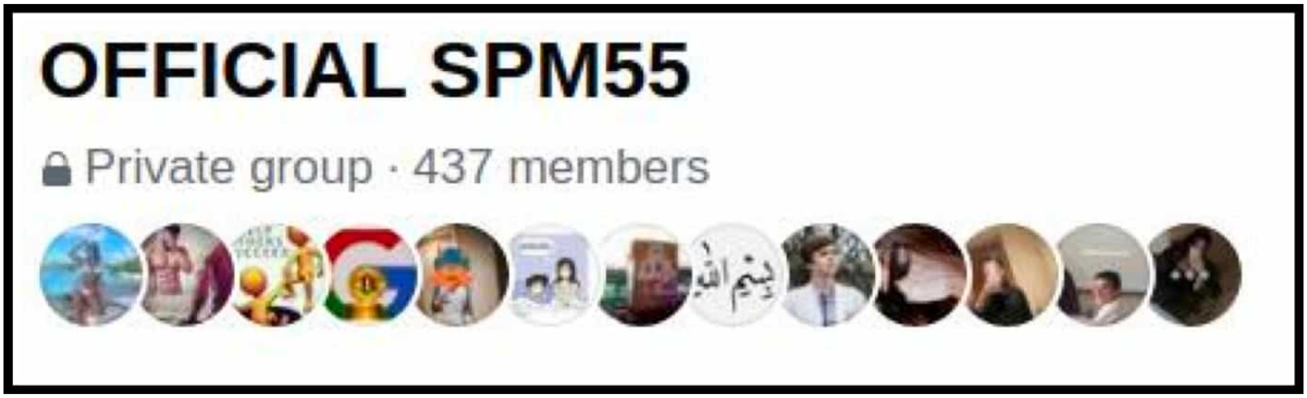
SPM55 operates out of Indonesia and its owner-admin uses the handle "AlexID" (among others). While AlexID is not the only SPM55 administrator, they appear to run the organization, as suggested by some of the earliest posts advertising the service which list them as the owner of SPM55 as well as developer comments addressed to "Alex" proposing how to approach technical questions.





```
window_width = $(window).width();

fixed_plugin_open = $('.sidebar .sidebar-wrapper .nav li.active a p').html();

if (window_width > 767 && fixed_plugin_open == 'Dashboard') {
  if ($('.fixed-plugin .dropdown').hasClass('show-dropdown')) {
    $('.fixed-plugin .dropdown').addClass('open');
  }

}

$('.fixed-plugin a').click(function(event) {
  // Alex if we click on switch, stop propagation of the event, so the dropdown will not be hide, otherwise we set the  section active
  if ($(this).hasClass('switch-trigger')) {
    if (event.stopPropagation) {
      event.stopPropagation();
    } else if (window.event) {
      window.event.cancelBubble = true;
    }
  }
});

$('.fixed-plugin .active-color span').click(function() {
  $full_page_background = $('.full-page-background');

  $(this).siblings().removeClass('active');
  $(this).addClass('active');

  var new_color = $(this).data('color');

  if ($sidebar.length != 0) {
    $sidebar.attr('data-color', new_color);
  }

  if ($full_page.length != 0) {
    $full_page.attr('filter-color', new_color);
  }

  if ($sidebar_responsive.length != 0) {
    $sidebar_responsive.attr('data-color', new_color);
  }
});
```

Increasingly suspicious of outsiders, this group is somewhat hesitant to do business with non-Indonesian speakers, much like how Russian cybercrime groups use idiomatic language as a kind of screening mechanism for prospective customers. SPM55 prefers payments using two Indonesian payments services, OVO and DANA, though they also accept Bitcoin and Ethereum. Even with this seemingly cautious approach to onboarding clients, the kits have found a receptive market and intelligence suggests customer accounts number in the several hundreds of active users with a sharp recent uptick in new customers.



OFFICIAL SPM55

🔒 Private group · 437 members

Infrastructure Associated With SPM55 and Actors

While some infrastructure associated with SPM55 is hosted in Indonesia, the client base cuts a wide swath across the globe with customers identified across in Nigeria, Pakistan, and other geographies also historically associated with phishing activity. In keeping with many such actors, there is a mix of both conventional domains registered for phishing attacks, as well as a strong reliance on dynamic DNS providers, given the ease with which such domains can be provisioned and the relatively lower cost and effort associated with abusing such services. We have included a set of IOCs related to SPM55 campaigns which highlight these and given the rate of recidivism of many SPM55 actors, pivots within registration information and passive DNS using Iris Investigate shows an even broader array of activity related to such actors.

Phishing remains to be the most common vector for account takeover and account fraud activity for many large organizations, contributing to significant financial losses as well as damage to brands as customers feel the impact of being victimized by these criminal services. Given their prevalence, continued evolution, and nexus of activity in the phishing-as-a-service marketspace, SPM55 is a criminal service worth keeping an eye on to help defend organizations and their customers against.

Recommendations

For companies and brands impacted by these phishing kits, monitoring for lookalike domains through solutions like DomainTools Detect can be an effective way of identifying and disrupting campaign infrastructure. The same applies to companies and brands that may become targets of this group in the future, given their frequent targeting pivots based on customer demand.

Use of passive DNS data is also helpful in identifying other domains used by actors to conduct this activity, including historical activity that may not have been previously observed to determine the rate of recidivism against a brand.

Submitting offending domains to Google Safe Browsing and other similar services can help prevent user and customer account fraud from compromised credentials.

```
onduties[.]com
eccoinbase[.]com
ycoinbase[.]com
tomlem[.]co[.]ke
recoveryaccount-alertcoinbaseconfirmation[.]4pu[.]com
nugroho-uwu[.]duckdns[.]org
job[.]oneplacement[.]com
verify-coinbase[.]cloudns[.]cl
usamanaeem[.]tech
sourcesexplore[.]com
dryousry[.]com
multandha[.]com
schooltv[.]in
thebonbon[.]hopto[.]org
uyoushop[.]com
www[.]siav[.]app
seuidcnetf[.]hopto[.]org
help[.]coinbaseaccsecruyh[.]com
https://voilas-store[.]com/
accountservices[.]sadte[.]net
heronationusa[.]com
securitycenter[.]name
test[.]zedtunefied[.]com
update[.]inteksplus[.]rs
authcoinbase[.]com
theabrasivepad[.]com
securerobinhood[.]com
ivenmo[.]com
Robinhood-help[.]com
upgradeservices[.]online/
servisess[.]com
recover-robinhood[.]com
actservc[.]com
cs-coiinbase[.]com
amzonconfirmaccountactivityupdate[.]ednbkxv[.]com
indra-ganteng[.]duckdns[.]org
jalanjalan[.]ddnsking[.]com
movismaps[.]com
https://naireport[.]com/
service-robinhooddsupportacount[.]duckdns[.]org
ferdiesoccermagic[.]com
www[.]kotapride[.]in
rcchilddevelopmentcentre[.]com
update-id-check[.]online
myproject[.]zzux[.]com
ngetes-sc-spm55[.]duckdns[.]org
https://www[.]fngs[.]in/
amazonsmilee[.]sytes[.]net
serv-actservicebilnaire[.]com
aptserv-sikat[.]com
secure-chasebanks[.]com
spm55-gadakobat[.]duckdns[.]org
tesbroo[.]com
hegar[.]com[.]mx
getazkaweb[.]com
```

```
ymailinfounusual[.]duckdns[.]org
sport5jarilah[.]duckdns[.]org
confirm[.]amz[.]update[.]account-id[.]sicrn[.]valid[.]database[.]uknown-information[.]iknasuf83g[.]co
mail-robinhoodsvice[.]servequake[.]com
jrcivils[.]co[.]uk
amazonservicesweb[.]myvnc[.]com
demo-robinhood[.]wikaba[.]com
cainbesecok[.]robin03[.]biz
revard[.]uz
auth-accounts-settings-policy[.]com
resolution-center-regarding-access[.]com
verify-identitycb[.]ddns[.]net
accoun-verifycb[.]ddns[.]net
verify-authsignin[.]duckdns[.]org
ap-robinhoodseic[.]servequake[.]com
identification-cb[.]ddns[.]net
encrypt3d[.]com[.]mx
secureappmailamzon[.]servequake[.]com
robbb[.]ddnsking[.]com
pen[.]serveftp[.]com
app-amznemailuseras[.]servequake[.]com
auth-restore-restricted-access[.]com
be-amzonseacureappmaile[.]serveuser[.]com
veri1fyacc0ount4amz[.]ns02[.]us
amzu-supporterervis[.]duckdns[.]org
web-apps[.]amazon[.]infosystem[.]cl
amazonfullupdate[.]serveuser[.]com
amzonaccounverif[.]serveusers[.]com
dontredagain[.]duckdns[.]org
coinbase[.]usps-care[.]us
foryoumeadlind[.]001www[.]com
redflagkntl[.]duckdns[.]org
em-suppsecureamz0neas[.]edns[.]biz
secure05c-chseonline[.]duckdns[.]org
cha-mailteamamzonea[.]serveuser[.]com
www3-pypalservice-resolvecenter[.]duckdns[.]org
makananenak[.]hopto[.]org
```