Fake sites stealing Steam credentials | Zscaler

By Prakhar Shrotriya

Published: 2020-02-11 · Archived: 2026-04-06 00:49:19 UTC

Recently, the Zscaler ThreatLabZ team came across multiple fake Counter-Strike: Global Offensive (CS:GO) skin websites aimed at stealing Steam credentials. These sites use an uncommon phishing technique that is difficult to detect. A similar campaign was seen in December 2019 and the campaign is still up with few enhancements, such as using a fake browser pop-up window for login along with some anti-analysis techniques, which are discussed in this blog.

Steam is a video game digital distribution service that provides automatic updates for various games. Steam has also expanded into an online web-based and mobile digital storefront. Steam offers digital rights management (DRM), matchmaking servers, video streaming, and social networking services, and it provides users with installation and automatic updates of games as well as several community features.

Steam is highly popular among gamers as it allows for multiplayer capabilities. How popular? According to statistics on the company website, the Steam platform has between 10 and 20 million concurrent users playing on any given day. At the time of this publication, the Steam site was showing more than 700,000 users currently playing CS:GO. The all-time peak number of concurrent users for CS:GO was 854,801.

Due to its popularity, the Steam platform has also become a popular target for attack. Cybercriminals will attempt to hijack a Steam account so they can launch other scams and attacks and steal or trade the victim's items.

The phishing site looks much like the real one. To make the phishing sites appear more legitimate, there is a fake chatbox with randomly selected phrases based on current events. The following screens show the phishing CS:GO site (top) and the actual CS:GO site (bottom).

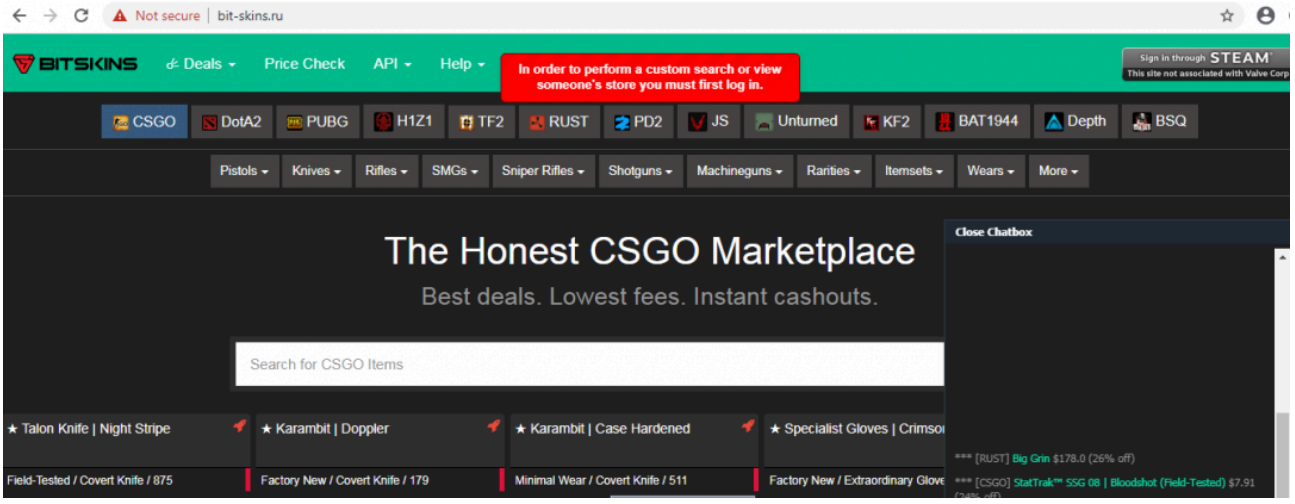

Figure 1: Phishing CS:GO site

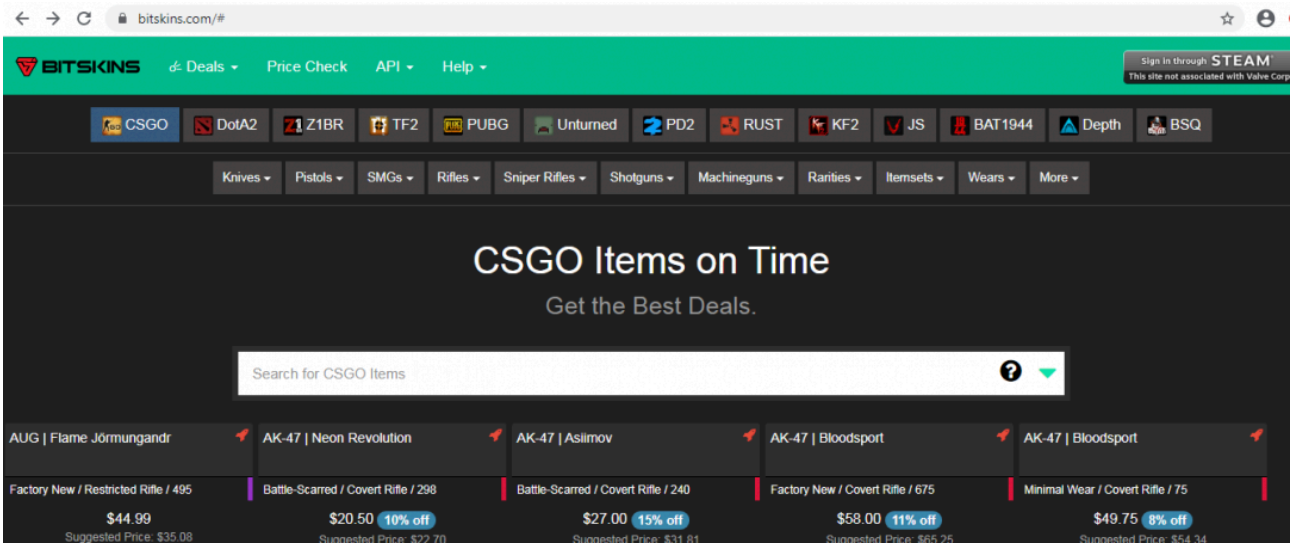

Figure 2: Legitimate CS:GO site

To perform a custom search or add items to a cart, users are asked to sign in with their Steam credentials. As the user clicks on the “Sign in through STEAM” button, a Steam login window pops up.

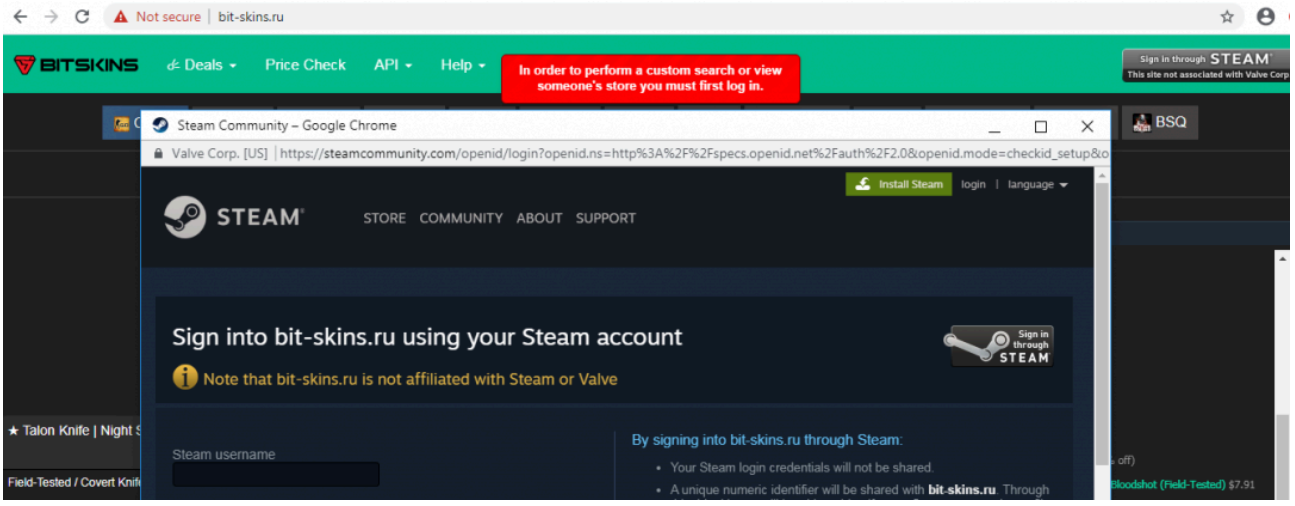

Figure 3: The Steam login window

Normally, the measures taken by a user to detect a phishing site include checking to see if the URL is legitimate, whether the website is using HTTPS, and whether there is any kind of homograph in the domain, among others.

In this case, everything looks fine as the domain is steamcommunity[.]com, which is legitimate and is using HTTPS. But when we try to drag this prompt from the currently used window, it disappears beyond the edge of the window as it is not a legitimate browser pop-up and is created using HTML in the current window.

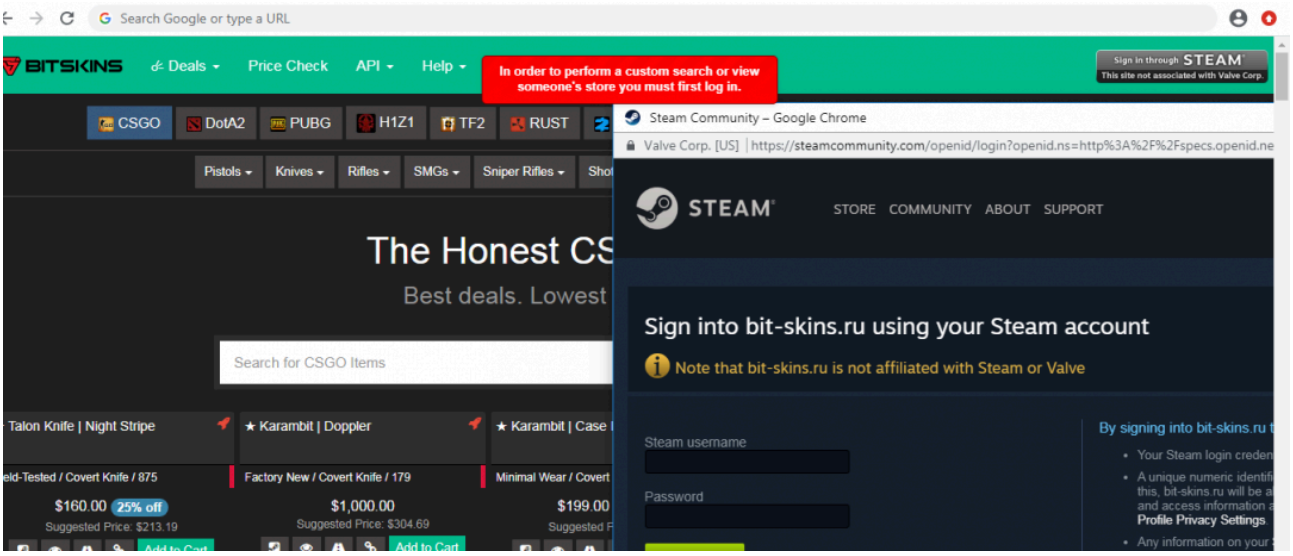

Figure 4: The fake browser pop-up window disappears beyond the edge

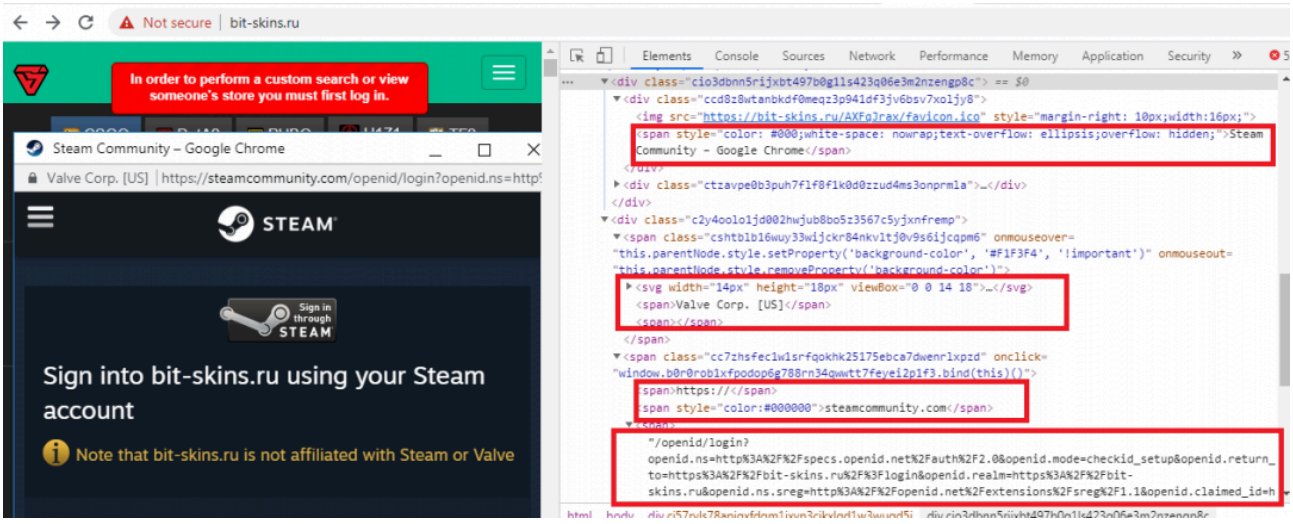

Figure 5: The fake browser pop-up window created using HTML

From the above screenshot, you can see that the browser header, address bar, and buttons to resize the window all are designed in HTML. Attackers have designed it precisely to make it look legitimate; for example, the color of the domain is slightly darker than the URI portion, and the color of the HTTPS part changes on mouseover.

When the victim clicks on the "Sign in through STEAM" button, the above discussed fake browser pop-up gets loaded from the below URL.

```
GET https://bit-skins.ru/jjfcPtYw/CG4OyNci76rr?domain=https%3A%2F%2Fbit-skins.ru&ref= HTTP/1.1
Host: bit-skins.ru
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Saf
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applicati
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: nested-navigate
Referer: https://bit-skins.ru/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: timezoneOffset=19800,0
```

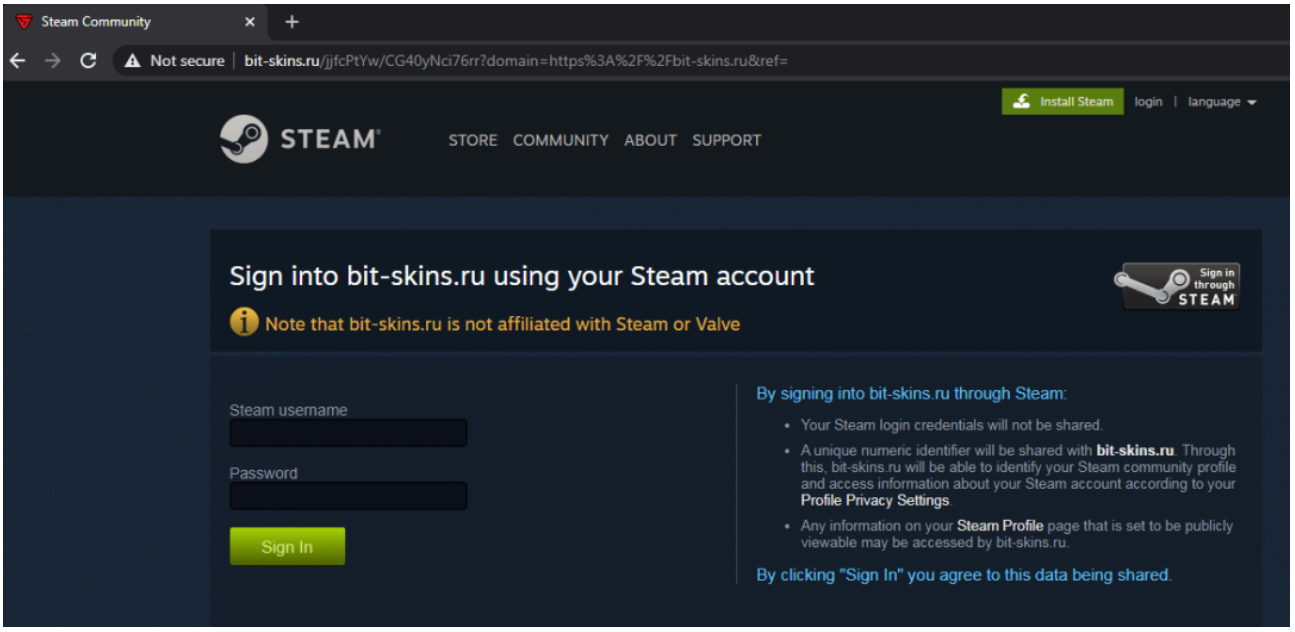

Figure 6: The fake Steam login page, which is used as a pop-up on the main page

If a user falls for this phishing and enters the login credentials, the credentials are sent to the attacker and the user is redirected to the legitimate site (hxxps://bitskins[.]com).

This phishing campaign also uses some anti-analysis techniques by detecting if the console is open in the browser. In this way, it prevents users from looking into the code directly. Below is the obfuscated JavaScript used to detect if the console is open.

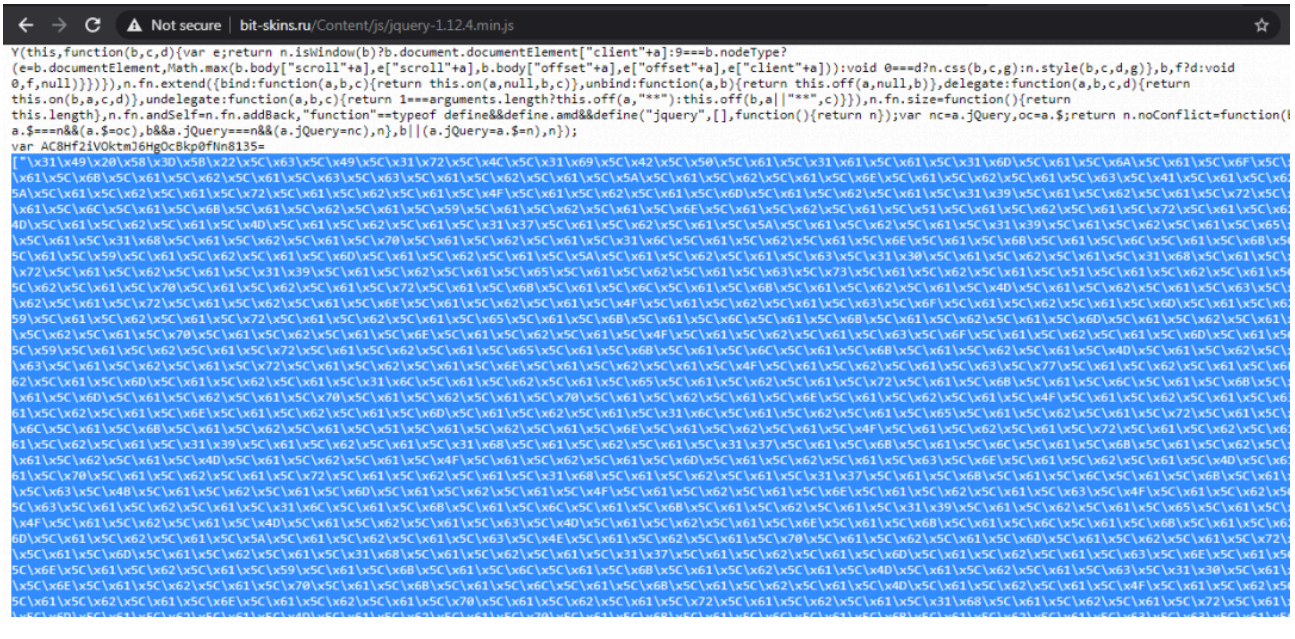

Figure 7: The obfuscated JavaScript to detect a browser console

After two levels of deobfuscation, we can see the script that detects whether the browser console is open. If it is open, the script activates a function, *debug322()*, which executes a "*debugger*" statement to stop the execution of the code.

```
    setInterval(function () {
        var _0x228dx5 = window.outerWidth - window.innerWidth > _0x228dx3,
            _0x228dx6 = window.outerHeight - window.innerHeight > _0x228dx3,
            _0x228dx7 = _0x228dx5 ? "vertical" : "horizontal";
        _0x228dx6 && _0x228dx5 || !(window.Firebug && window.Firebug.chrome && window.Firebug.chrome.isInitialized ||
        _0x228dx5 || _0x228dx6) ? (_0x228dx2.open && _0x228dx4(!1, null), _0x228dx2.open = !1, _0x228dx2.orientation = null) :
          (_0x228dx2.open && _0x228dx2.orientation === _0x228dx7 || _0x228dx4(!0, _0x228dx7), _0x228dx2.open = !0,
        _0x228dx2.orientation = _0x228dx7)
    }, 500), "undefined" != typeof module && module.exports ? module.exports = _0x228dx2 : window.devtools = _0x228dx2
}(), window.addEventListener("devtoolschange", function (_0x228dx2) {
    if (!0 === _0x228dx2.detail.open) {
        var _0x228dx3 = setInterval(function () {
            !0 === window.devtools.open ? debug322() : clearInterval(_0x228dx3)
        }, 1);
        debug322()
    }
})
```

Figure 8: The deobfuscated code to detect the browser console

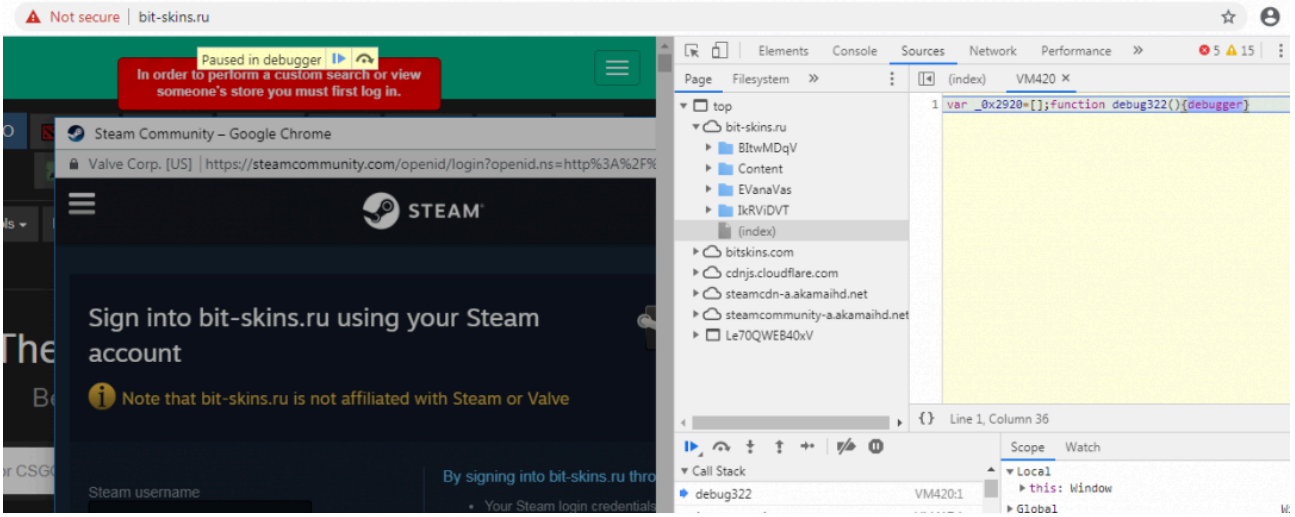

Figure 9: The execution of the "debugger" statement as the console is opened

As of now, ThreatLabZ has detected more than 200 domains as part of this campaign, and there are multiple other templates used in this campaign with similar functionalities, as discussed above.

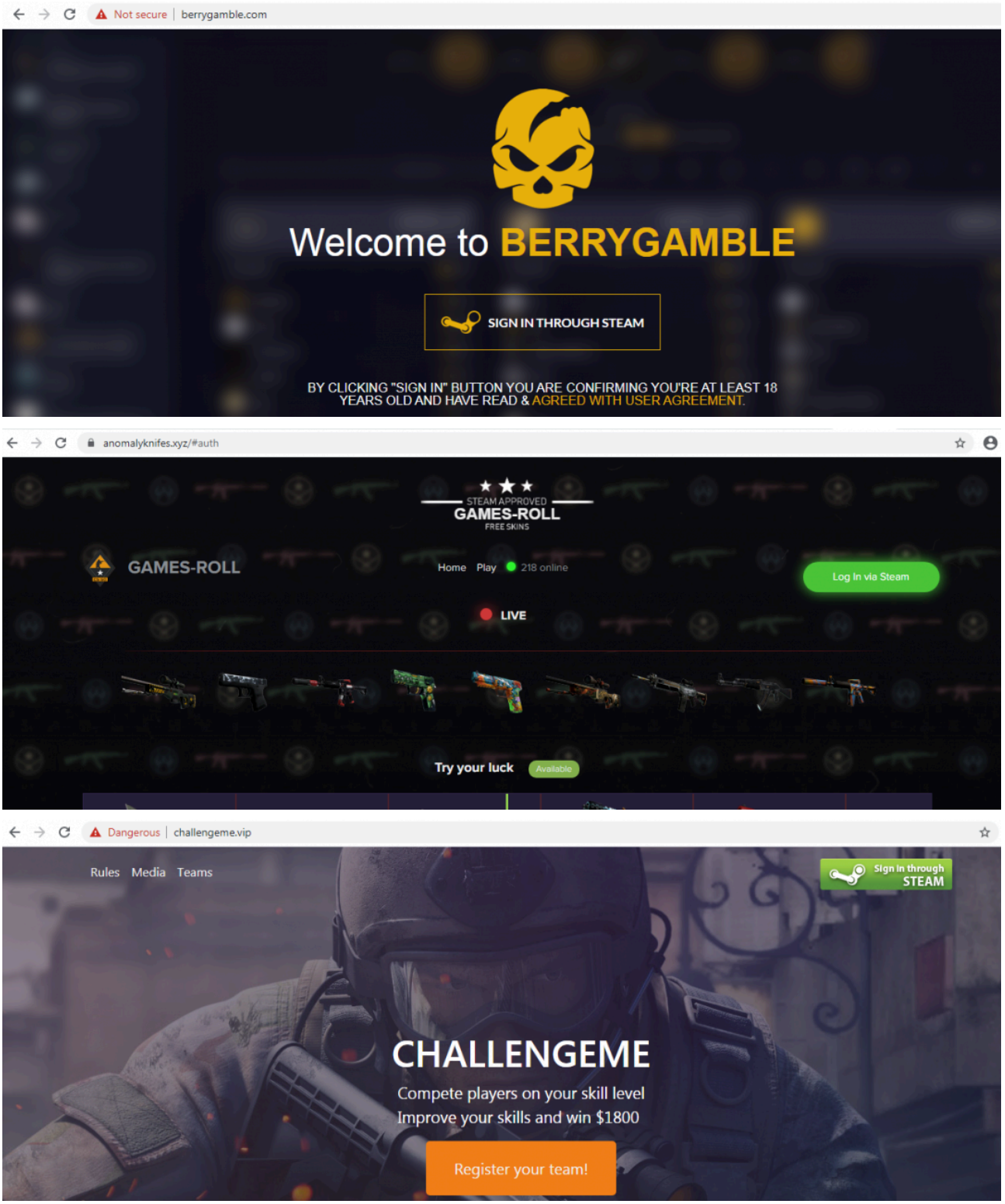

Figure 11: Some of the different templates used in this campaign

Conclusion

Phishing campaigns are getting more sophisticated day by day, and attackers are using new and lesser-known techniques in these campaigns. Most of the common checks that a user does before entering the login credentials

to any website may not work in this campaign, such as checking the domain, use of HTTPS, etc. The Zscaler ThreatLabZ team is actively working on detecting and providing coverage from such attacks.

As always, our best advice to protect yourself is to only log in to Steam directly from the steampowered.com domain. If you are using another site that wants to log in through Steam, be sure to thoroughly research the site before entering any login credentials.

IOCs

aladdinhub[.]fun
allskinz[.]xyz
ano-skinspin[.]xyz
anomalyknifes[.]xyz
anomalyskin[.]xyz
anomalyskinz[.]xyz
anoskinzz[.]xyz
berrygamble[.]com
bit-skins[.]ru
bitknife[.]xyz
bitskines[.]ru
challengeme[.]vip
challengeme[.]in
challengme[.]ru
cmepure[.]com
cmskillcup[.]com
counterpaid[.]xyz
counterspin[.]top
counterstrikegift[.]xyz
cs-beast[.]xyz
cs-lucky[.]xyz
cs-pill[.]xyz
cs-prizeskins[.]xyz
cs-prizeskinz[.]xyz
cs-simpleroll[.]xyz
cs-skinz[.]xyz
cs-smoke[.]xyz
cs-spinz[.]xyz
cs-victory[.]xyz
csallskin[.]xyz
csbuyskins[.]in
cscoat[.]eu
csgo-analyst[.]com
csgo-cash[.]eu

csgo-steamanalyst[.]net
csgo-swapskin[.]com
csgo-trade[.]net
csgo-up[.]com
csgobeats[.]com
csgocase[.]one
csgocashs[.]com
csgocheck[.]ru
csgocompetive[.]com
csgodetails[.]info
csgodreamer[.]com
csgodrs[.]com
csgoelite[.]xyz
csgoencup[.]com
csgoevent[.]xyz
csgoindex[.]ru
csgoitemdetails[.]com
csgoitemsprices[.]com
csgoko[.]tk
csgomarble[.]xyz
csgomarketplace[.]net
csgomarkets[.]net
csgoprocupgo[.]com
csgorcup[.]com
csgorose[.]com
csgoroyalskins1[.]com
csgoskill[.]ru
csgoskinprices[.]com
csgoskinsinfo[.]com
csgoskinsroll[.]com
csgosteamanalysis[.]com
csgosteamanalyst[.]ru
csgoteammate[.]gq
csgothunby[.]com
csgotrades[.]net
csgovip[.]ru
csgoxgiveaway[.]ru
csgozone[.]net[.]in
csgunskins[.]xyz
csmoneyskinz[.]xyz
csmvcecup[.]com
csprices[.]in

csskillpro[.]xyz
csskinz[.]xyz
cstournament[.]ru
csxrnoney[.]com
cybergamearena[.]ru
d2cups[.]com
d2faceit[.]com
deamonbets[.]ru
demonbets[.]ru
diablobets[.]com
doatgiveaway[.]top
dopeskins[.]com
dota2fight[.]ru
dota2fight[.]net
dota2giveaway[.]top
dota2giveaways[.]top
dotafights[.]vip
dotagiveaway[.]win
earnskinz[.]xyz
emeraldbets[.]ru
esportgaming[.]ru
event-games4roll[.]com
exchangeuritems[.]gq
extraskinscs[.]xyz
ezwin24[.]ru
faceiteasyleague[.]ru
fireopencase[.]com
free-skins[.]ru
game4roll[.]com
gameluck[.]ru
games-roll[.]ru
games-roll[.]ml
games-roll[.]ga
giveawayskin[.]com
global-skins[.]gq
globalcsskins[.]xyz
globalskins[.]tk
goldendota[.]com
goodskins[.]gq
gosteamanalyst[.]com
gtakey[.]ru
hellgiveaway[.]trade

hltvcsgo[.]com
hltvgames[.]net
knifespin[.]top
knifespin[.]xyz
knifespin[.]top
knifespins[.]xyz
knifez-roll[.]xyz
knifez-win[.]xyz
league-csgo[.]com
lehatop-01[.]ru
loungeztrade[.]com
lucky-skins[.]xyz
makson-gta[.]ru
maxskins[.]xyz
mvcsgo[.]com
mvpcup[.]ru
mvptournament[.]com
mygames4roll[.]com
night-skins[.]com
ownerbets[.]com
playerskinz[.]xyz
rangskins[.]com
roll-skins[.]ru
roll4knife[.]xyz
rollknfez[.]xyz
rollskin-simple[.]xyz
csgo-market[.]ru[.]com
sakuralive[.]ru[.]com
csgocupp[.]ru[.]com
csgoeasywin[.]ru[.]com
csgocybersport[.]ru[.]com
csgocheck[.]ru[.]com
csgo-market[.]ru[.]com
csgoindex[.]ru[.]com
rushbskins[.]xyz
rushskins[.]xyz
s1mple-spin[.]xyz
simple-knifez[.]xyz
simple-win[.]xyz
simplegamepro[.]ru
simpleroll-cs[.]xyz
simplespinz[.]xyz

simplewinz[.]xyz
skin-index[.]com
skin888trade[.]com
skincs-spin[.]xyz
skincs-spin[.]top
skinmarkets[.]net
skins-hub[.]top
skins-info[.]net
skins-jungle[.]xyz
skinsboost[.]ru
skinsdatabse[.]com
skinsind[.]com
skinsmind[.]ru
skinspace[.]ru
skinsplane[.]com
skinsplanes[.]com
skinsplanets[.]com
skinxmarket[.]site
skinz-spin[.]top
skinz-spin[.]xyz
skinzjar[.]ru
skinzprize[.]xyz
skinzspin-cs[.]xyz
skinzspinz[.]xyz
spin-games[.]com
spin4skinzcs[.]top
spin4skinzcs[.]xyz
spinforskin[.]ml
sponsored-simple[.]xyz
staffstatsgo[.]com
starrygamble[.]com
stat-csgo[.]ru
stats-cs[.]ru
steam-analyst[.]ru
steamanalysts[.]com
steamgamesroll[.]ru
stewie2k-giveaway-150days[.]pro
sunnygamble[.]com
swapskins[.]live
test-domuin2[.]com
test-domuin3[.]ru
test-domuin4[.]ru

test-domuin5[.]ru
tournamentt[.]com
waterbets[.]ru
ultimateskins[.]xyz
win-skin[.]top
win-skin[.]xyz
winknifespin[.]xyz
winskin-simple[.]xyz
winskins[.]top
wintheskin[.]xyz

Source: https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials