Investigation of a Long-Lived Phishing Kit

seclarity.io/resources/blog/the-art-of-perswaysion-phishing-kit/

The Art of PerSwaysion

Executive Summary

Phishing kits are some of the most powerful enablers of digital crime. By having a cookie-cutter, ready-made format that can be purchased by anyone, the barrier to entry in creating convincing fake login portals is nearly eliminated. There have been several reports in recent months (TodayZoo

Franken-phish: TodayZoo built from other phishing kits. October 21, 2021. Accessible here.

, most recently) that point out attacks leveraging phishing kits. This report investigates a kit that has stayed active for more than four years. In just the last 18 months, thousands of users across more than a dozen public and private sectors are known to have been affected, suggesting that this kit has had a tremendous impact on organizations far and wide.

Uncovering the Activity

Author's Note

I'd like to add a disclaimer here before continuing. This section starts with a bit of a marketing vibe to it, but this is really how it happened. Feel free to skip this part of the narrative.

In late October, I sat down to start creating useful content for a new platform my team and I are launching called NetworkSage. One of the first technical blogs I wrote focuses on how various Sandbox technologies -- while incredibly useful -- have some important gaps that are addressed by NetworkSage (if interested, you can read that blog post here). While collecting data and finishing up one of the key points I was making (*Scenario 5: User Visits Known Phishing Site*), I realized that I was actively staring at something that

shared attack infrastructure with a number of other samples in our system:

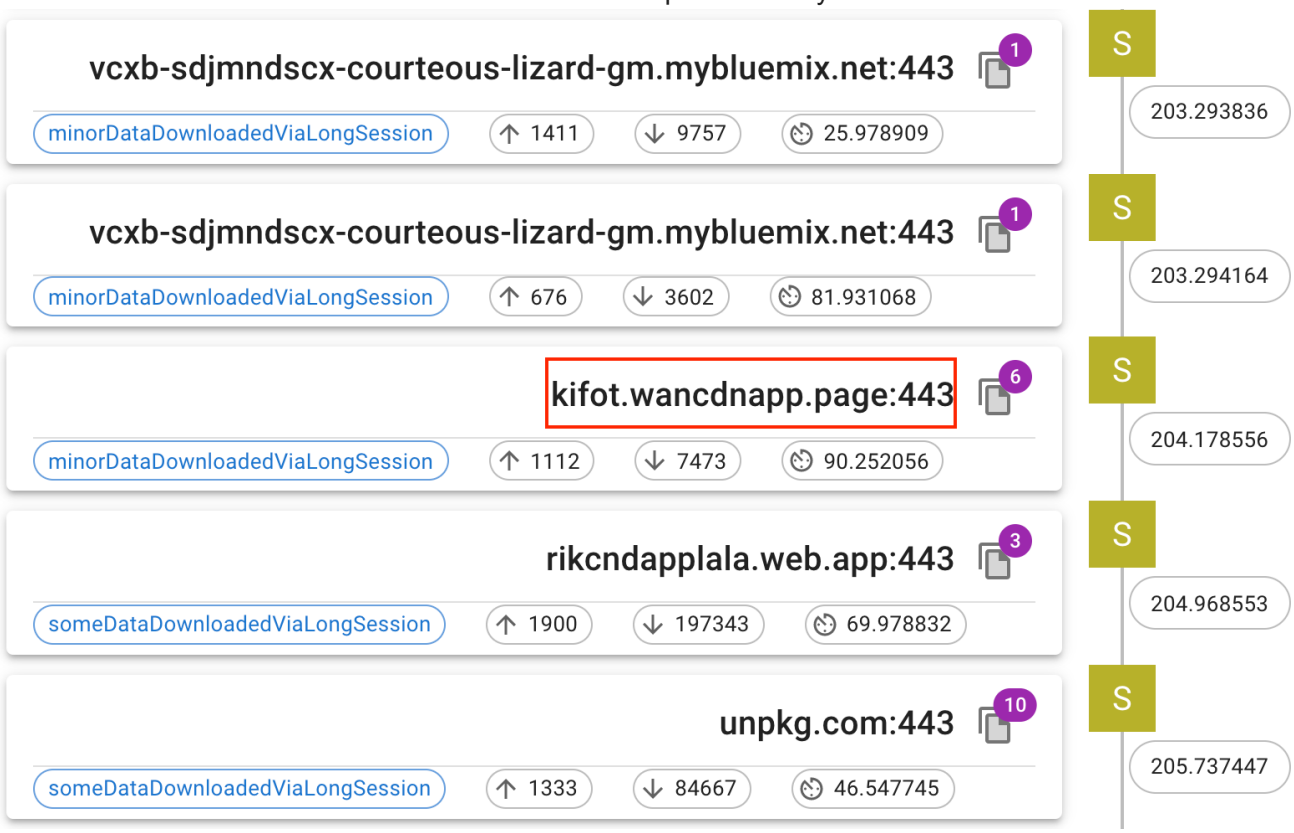


Figure 1: Suspicious Domain Appearing in Several Samples

Further still, I noticed that there was another domain showing up soon after the above activity. This appeared to be occurring in all of the samples where I entered credentials into the site, and almost always had a C2-like channel associated with it:

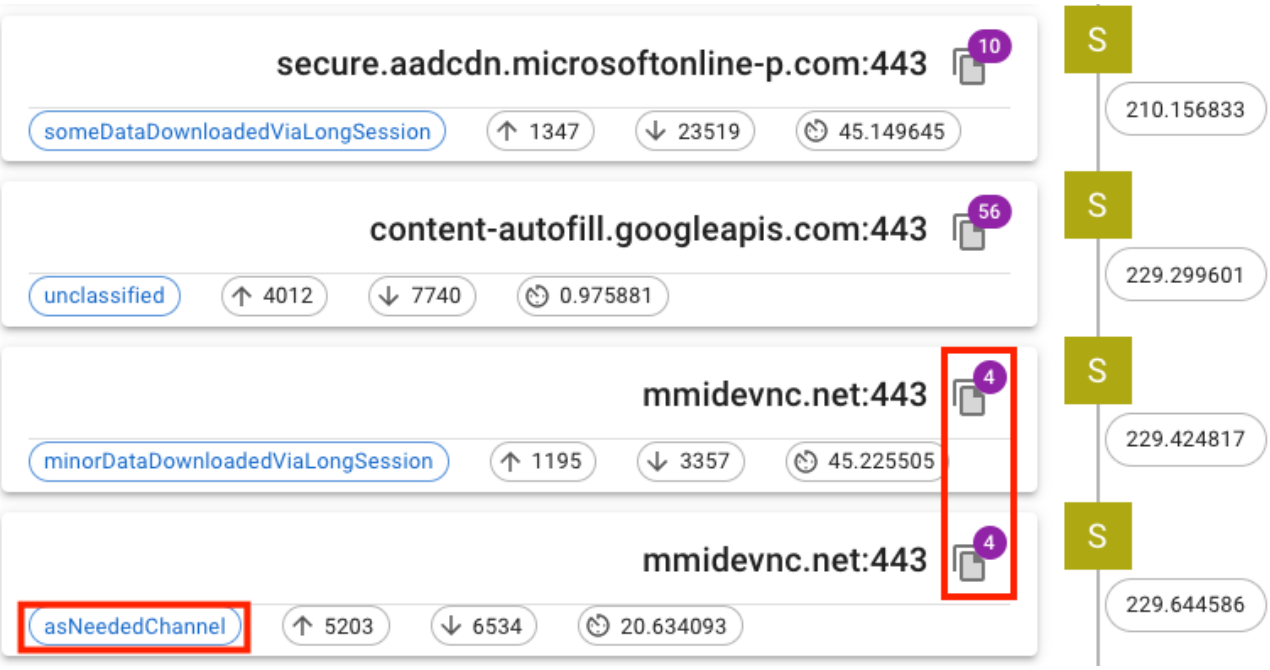


Figure 2: Suspicious Domain with C2-like Behavior

This discovery led me to the hypothesis that there was a widespread attack occurring that was flying under the radar of most systems.

Previous Reporting

Before getting into the technical details, I want to note that about half-way into my investigation, I discovered that portions of this attack and group (dubbed *PerSwaysion*) had been found and reported on previously. Interestingly, despite these reports, the activity has continued uninterrupted. In January of 2020, Avanan researchers briefly discussed one particular tactic used by clients of the phishing kit, namely the delivery of exceptionally legitimate-looking emails that link to malicious content hosted on Microsoft's Sway service

Cybercriminals Use Microsoft Sway Scams to Phish Office 365 Security and Your Well-Trained Users. January 9, 2020. Accessible here.

. This provided a bit of context about how attackers use Microsoft Sway to bypass security filters and convince users that their request is legitimate.
In April of 2020, Group-IB did a much deeper dive

PerSwaysion Campaign: Playbook of Microsoft Document Sharing-Based Phishing Attack. April 30, 2020. Accessible here.

. Their report laid out a narrative that:

- dubbed the group *PerSwaysion*
- laid out the arc of events as they knew it (spanning from August 2019 through April 2020)
- identified the likely nationality of the developers of the kit (Vietnamese)
- described the kit's global customer base
- established some aspects of the modularity of the kit
- provided a detailed review of some aspects of the attacker infrastructure
- gave a walkthrough of a particular compromise
- discussed known victim locations and relevance
- identified some artifacts that can be used to find these attacks

These are both great reports that I recommend reviewing. As such, I will not repeat content that they have already covered. Instead, in this report I'll spend time:

- establishing the overall timeline of the group, which actually extends back to 2017
- describing activity since the last report, including the scope of victims
- elaborating on aspects of the kit not yet discussed
- identifying Attack Vectors
- identifying indicators userful for hunting and detection at various stages of the attack
- providing a way to determine if you've been affected

Throughout this report I will also describe how I found much of this information. I believe this is an important contribution for the benefit of the security community beyond just this report. What follows is the investigation and how it unfolded.

Understanding the Scope

The system we're releasing today is new and focuses on network traffic, which is absolutely critical for understanding activity when it's hard or impossible to reproduce. However, because this attack was ongoing, I chose to investigate further by analyzing my samples and correlating them with Urlscan, a community platform focused on detonating URLs. This allowed me to dig deeper into what was actually happening in each of these steps.I had many questions, but two were crucial to answer in order to determine the attack's scope.

Question 1: How Long has the Attack Existed?

While trying to establish the timeline for this attack, I first needed to understand how many samples existed using the domain that originally piqued my curiosity -- `wancdnapp[.]page`. Using Urlscan's search feature, I was able to quickly get an idea of how many samples contained it:

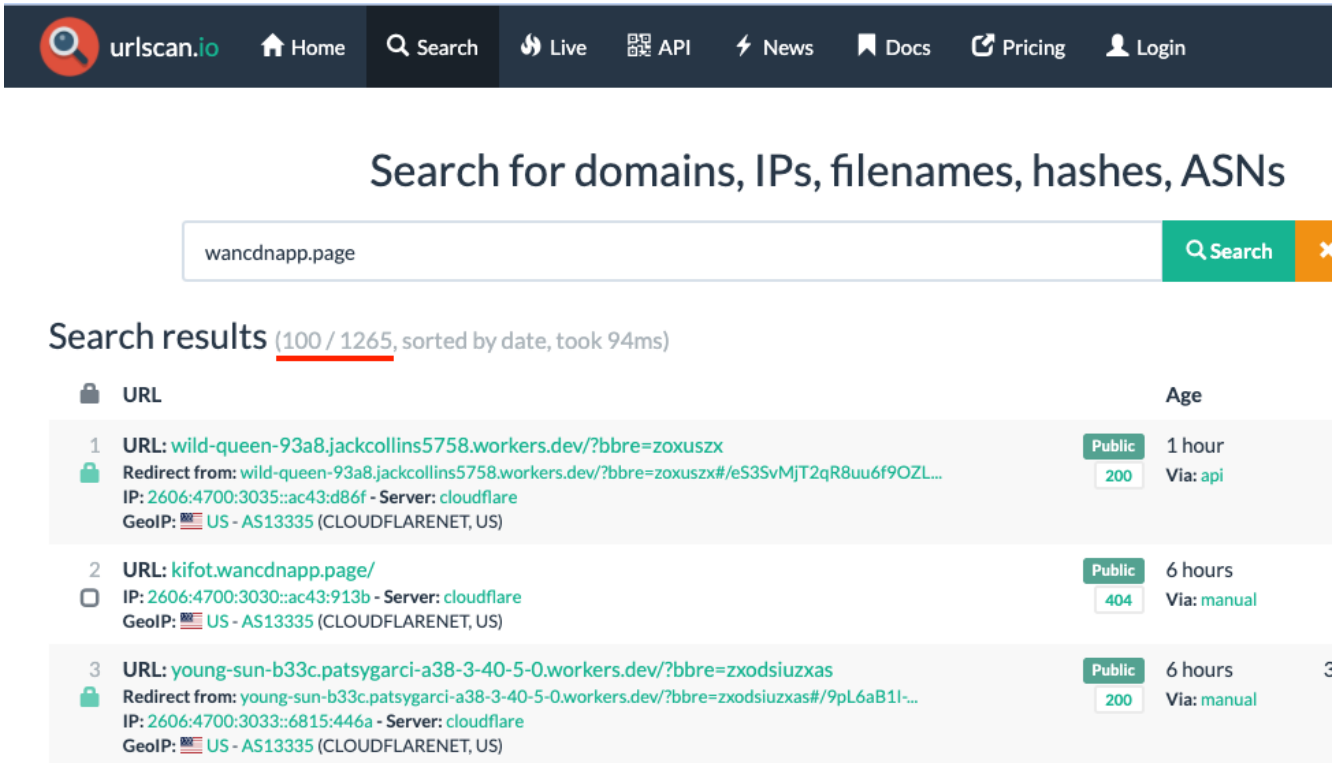


Figure 3: Discovering How Many Samples had Suspicious Domain

From there, I was able to review the samples and analyze the files requested from various submissions over time. I correlated this with manual analysis I was performing on live phishing portals, further

cementing the similarity of activity across time:

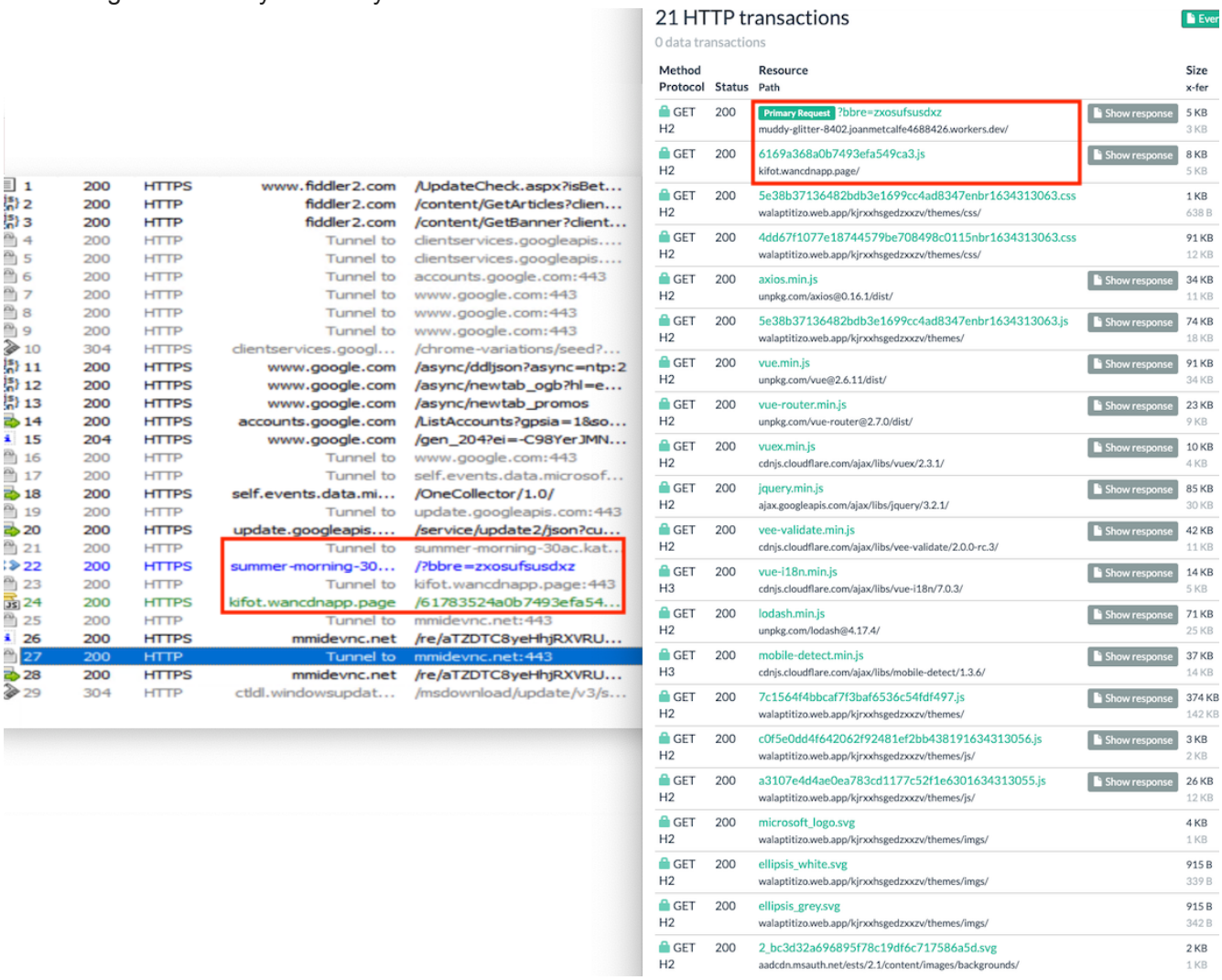


Figure 4: Comparing Data Between Fiddler and Urlscan

The next step involved analysis of several of the Javascript files referenced in the chain of requests that lead to a rendered phishing portal.

Javascript Analysis

In all known cases, these Javascript files are found within a `themes` directory (more on this later). By analyzing samples that have that structure and share other similarities, it was possible to discover that this activity spanned far into the past. Interestingly, some samples' Javascript files are packed, while others are not. However, once compared in unpacked form, the code reuse is quite significant. As an example, below

is an excerpt of the comparison of two samples from November 2019 and November 2021:

```
7178     path: '/vi/*',
7179     name: 'error404-vi',
7180     meta: {
7181         lang: 'vi'
7182     },
7183     component: function(resolve, reject) {
7184         loadComponent('error404',
7185-            'themes/js/c0f5e0dd4f642062f92481ef2bb438191574786424.js'
7186             ).then(resolve, reject);
7187     }
7188-}, {
7189     path: '/*',
7190     name: 'error404-en',
7191     meta: {
7192         lang: 'en'
7193     },
7194     component: function(resolve, reject) {
7195         loadComponent('error404',
7196-            'themes/js/c0f5e0dd4f642062f92481ef2bb438191574786424.js'
7197             ).then(resolve, reject);
7198     }
7199-}, ];
7200 var PAGE_TITLE = {
7201     "Home-en": "Your Dashboard",
7202     "Foo-en": "About Us Page",
7203     "Bar-en": "About Us Page",
7204     "Error-en": "Error:Page not found"
7205 };
7206 var __dirname = "";
7207 var ch4kbat = "0";
7208 var validStepUlg = "1";
7209
7210 function closeOpenwinnbr(url) {
7211     window.opener.location.href = url;
7212     self.close();
7213 }
7214 var router = new VueRouter({
```

```
16106             path: '/vi/*',
16107             name: 'error404-vi',
16108             meta: {
16109                 lang: 'vi'
16110             },
16111             component: function(resolve, reject) {
16112                 loadComponent('error404',
16113+                    'themes/js/c0f5e0dd4f642062f92481ef2bb438191634313056.js'
16114                     ).then(resolve, reject);
16115             }
16116+        },
16117+        {
16118             path: '/*',
16119             name: 'error404-en',
16120             meta: {
16121                 lang: 'en'
16122             },
16123             component: function(resolve, reject) {
16124                 loadComponent('error404',
16125+                    'themes/js/c0f5e0dd4f642062f92481ef2bb438191634313056.js'
16126                     ).then(resolve, reject);
16127             }
16128+        },
16129+    ];
16130     var PAGE_TITLE = {
16131         "Home-en": "Your Dashboard",
16132         "Foo-en": "About Us Page",
16133         "Bar-en": "About Us Page",
16134         "Error-en": "Error:Page not found"
16135     };
16136     var __dirname = "";
16137     var ch4kbat = "0";
16138     var validStepUlg = "1";
16139
16140     function closeOpenwinnbr(url) {
16141         window.opener.location.href = url;
16142         self.close();
16143     }
16144     var router = new VueRouter({
```

Figure 5: Code Comparison of Two Samples

However, not everything is identical. While analyzing scripts for one of the samples, I found a reference to a domain name that only exists in a comment:

```
3305     return VueHtml5Editor;
3306 })); //anytools.biz app dev 2019
3307 var makeCRCNBR = function() {
3308     var c;
3309     var crcTable = [];
3310     for (var n = 0; n < 256; n++) {
3311         c = n;
3312         for (var k = 0; k < 8; k++) {
3313             c = ((c & 1) ? (0xEDB88320 ^ (c >>> 1)) : (c >>> 1));
3314         }
3315         crcTable[n] = c;
3316     }
3317     console.log("CREATED");
3318     return crcTable;
3319 };
```

Figure 6: Domain Name in Code Comment

Searching for this domain led me to discover that the same comment existed in a piece of code that was uploaded to a Javascript hosting platform in August of 2019:

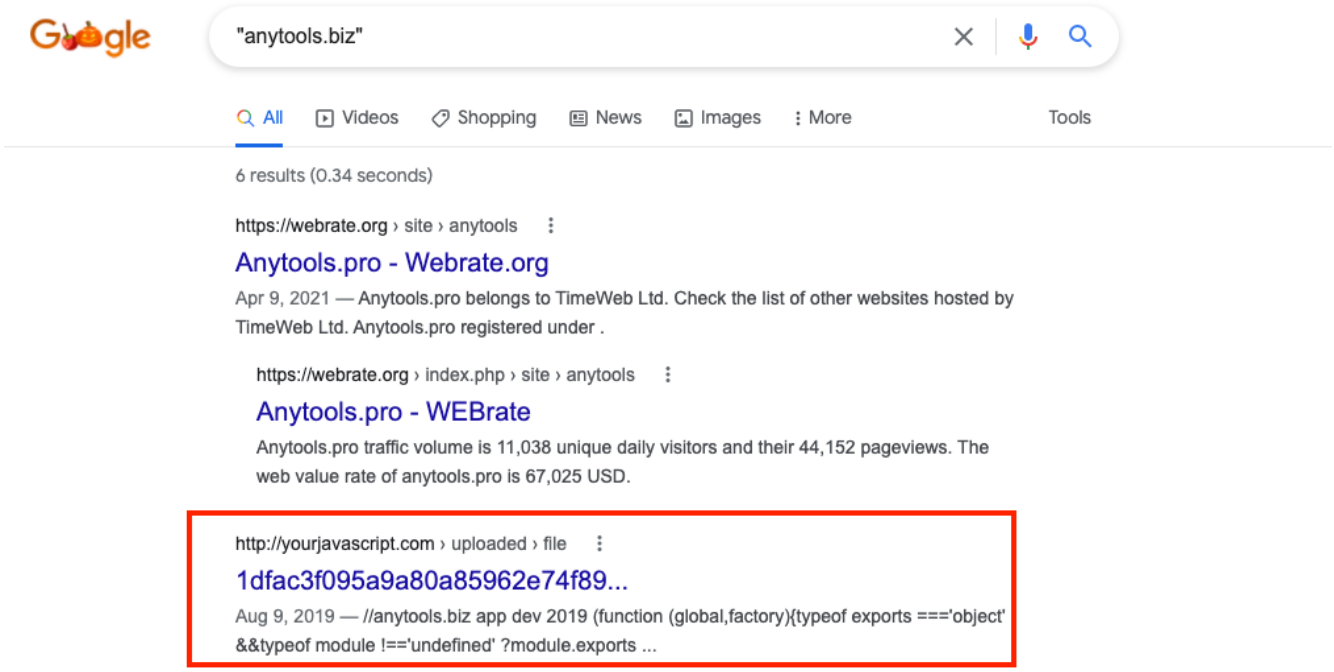


Figure 7: Script Found on Javascript Hosting Platform

By refining the search to both topics, I was able to learn which user uploaded the file:

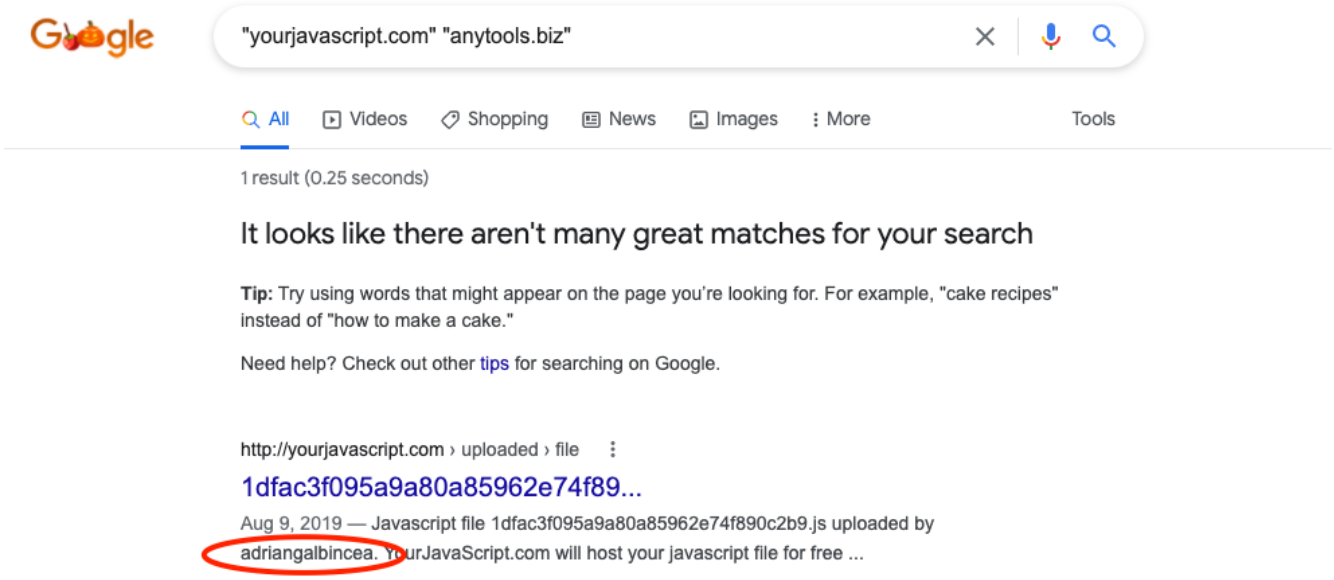


Figure 8: User Associated with Script

At this time, I became aware of the Group-IB report (and consequently the Avanan report), namely because the researchers at Group-IB found this exact same link! However, this was the earliest activity that they confidently identified as part of this phishing kit.Returning to my discovery of the `anytools[.]biz` reference, I noticed (via its WHOIS information) that it was registered nearly **two years earlier** than this

established start of activity:

```
>>> Last update of WHOIS database: 2021-10-31T13:52:19Z <<<

# whois.google.com

Domain Name: anytools.biz
Registry Domain ID: D264169086BA246BF80F689893AE426B4-NSR
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2018-06-10T09:50:20Z
Creation Date: 2017-09-23T10:49:12Z
Registrar Registration Expiration Date: 2027-09-23T10:49:12Z
Registrar: Google LLC
Registrar IANA ID: 895
```

Figure 9: WHOIS for anytools[.]biz

While sophisticated adversaries certainly use the concept of domain aging

Domain aging is the process of registering a domain much earlier than when it will be used in an attack. For details, review page 18 of APWG's *Global Phishing Survey: Trends and Domain Name Use in 2016*, which is available here.

, I was highly suspicious that this domain lay dormant for so long.

A Pattern Emerges

At this point, I spent several hours researching characteristics that identified other related activity. Reviewing some samples with similar URL parameters, for example, led to additional domains I had not yet discovered (such as this one), which associated domain perfectstuff[.]info to the attack). Others had PHP script names that were relatively unique, such as `1.newsvpost_ads/loading.php`. Searching the Internet for that string led me to this Pastebin paste identifying domain `sptech[.]org`. Finally, after reviewing the known Credential Collection site from the Group-IB report (`c3y5-tools[.]com`), I noticed that a considerable number of the attack domains had similar registration dates clustered around late

September of 2017:

```
# whois.afilias.net

Domain Name: PERFECTSTUFF.INFO
Registry Domain ID: D503300000045679323-LRMS
Registrar WHOIS Server:
Registrar URL: https://domains.google.com
Updated Date: 2018-06-10T19:40:06Z
Creation Date: 2017-09-24T01:54:39Z
Registry Expiry Date: 2027-09-24T01:54:39Z
Registrar Registration Expiration Date:
Registrar: Google LLC
Registrar IANA ID: 895
```

```
# whois.google.com

Domain Name: c3y5-tools.com
Registry Domain ID: 2168478702_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2019-11-12T07:59:59Z
Creation Date: 2017-09-28T18:39:33Z
Registrar Registration Expiration Date: 2027-09-28T18:39:33Z
Registrar: Google LLC
Registrar IANA ID: 895
```

```
>>> Last update of WHOIS database: 2021-11-01T19:34:45Z <<<

# whois.google.com

Domain Name: sptech.org
Registry Domain ID: D402200000003758343-LROR
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2019-06-04T18:14:21Z
Creation Date: 2017-09-29T03:13:23Z
Registrar Registration Expiration Date: 2027-09-29T03:13:23Z
Registrar: Google LLC
Registrar IANA ID: 895
```

Figure 10: Cluster of Domains with Similar Creation Date

This matched closely in time with the registration of `anytools[.]biz`, which further strengthened my suspicion that mid 2019 was **not** the beginning of the attack.

A Breakthrough

On the last day of intelligence gathering, I was able to definitively tie the activity all the way back to October 10, 2017. This was made possible by the community of Urlscan users who share links they've received in exchange for better knowledge about whether it is malicious. Without this community and this platform, I likely never would have confirmed my suspicion.

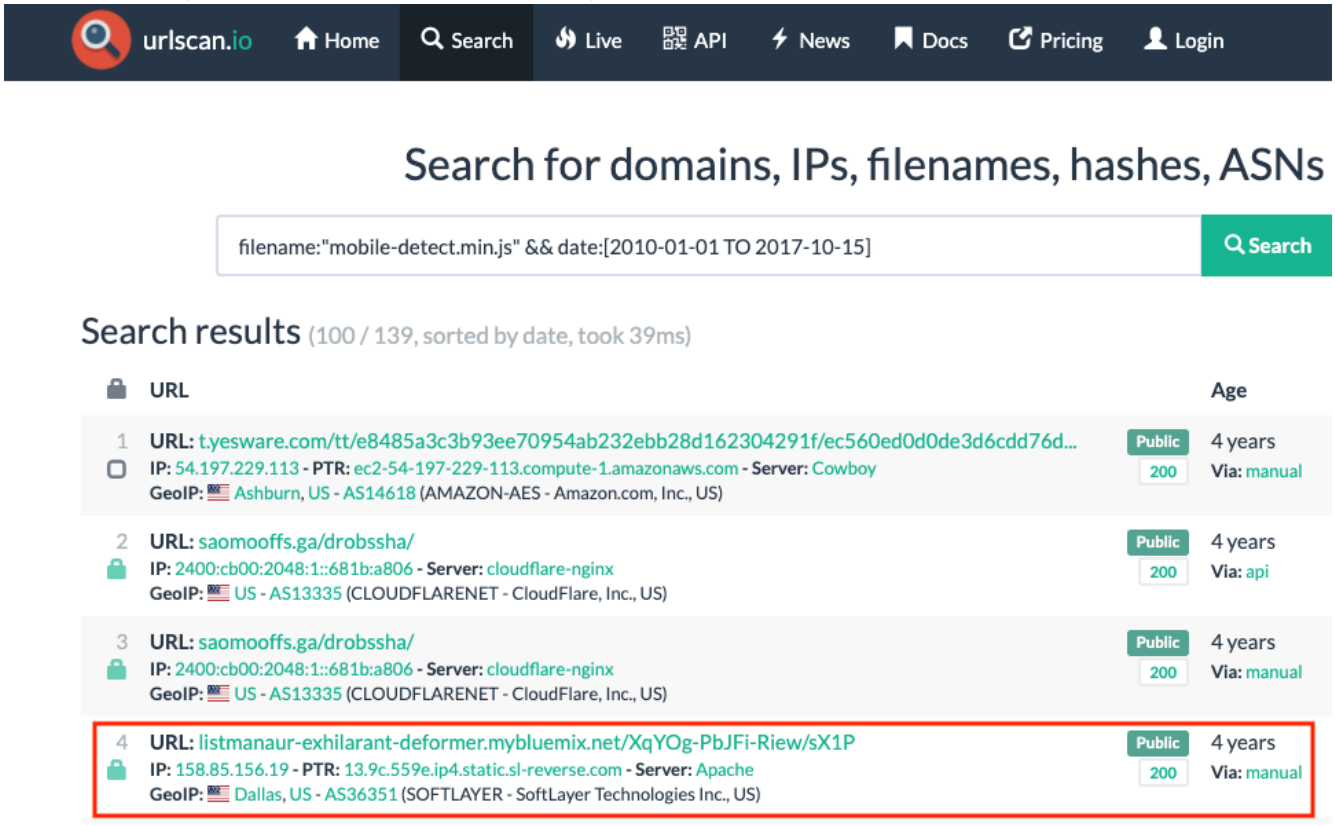
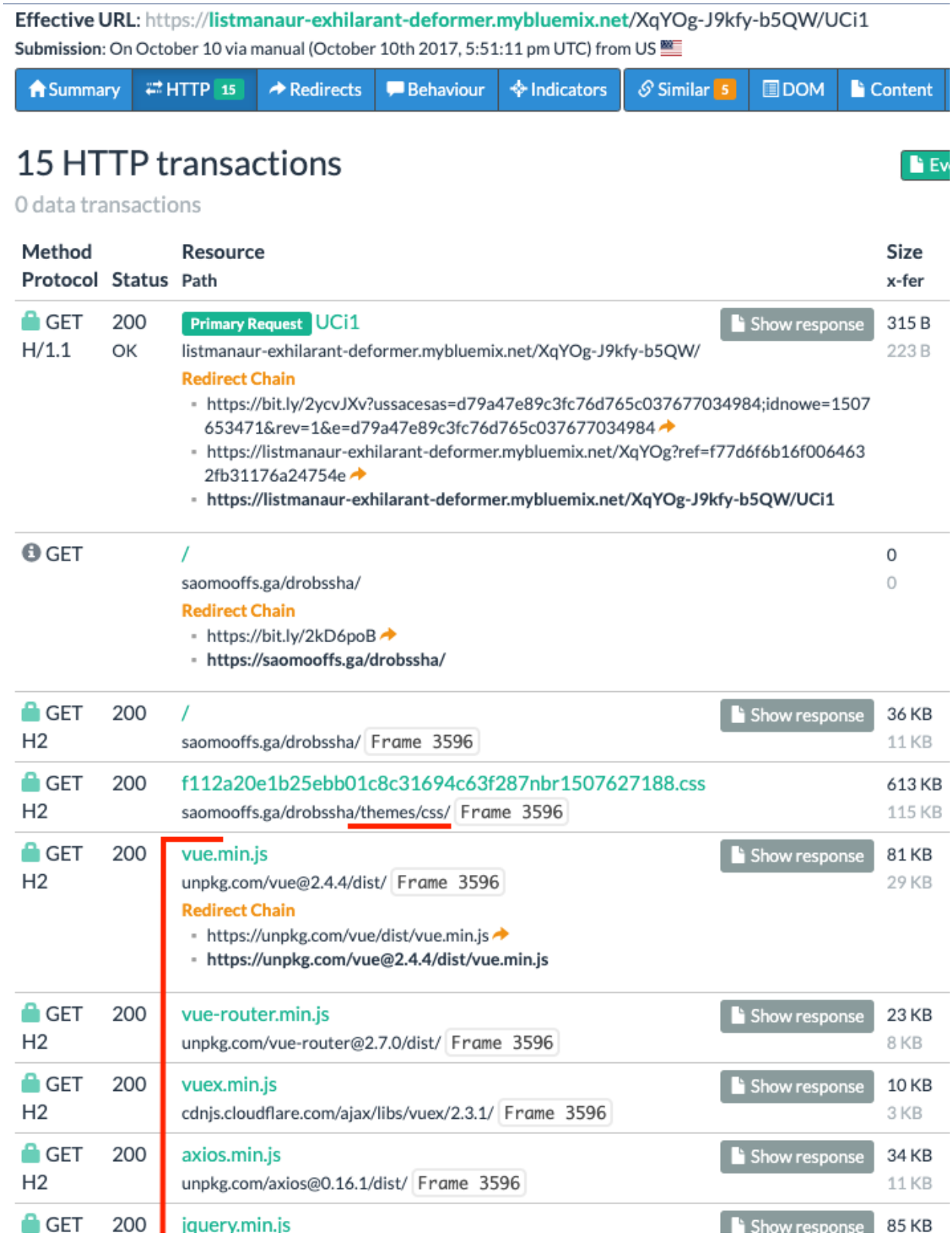


Figure 11: Finding the Oldest Known Sample

The connection was made by first identifying something that **all** samples have in common (loading `mobile-detect.min.js`, a benign and open-source library), iteratively searching for all submissions that contained that file, and then reviewing the sequence of events that occurred during that site's loading. While this may not be the actual beginning of the attack, it serves as the earliest-known use of the TTPs I'll describe later:



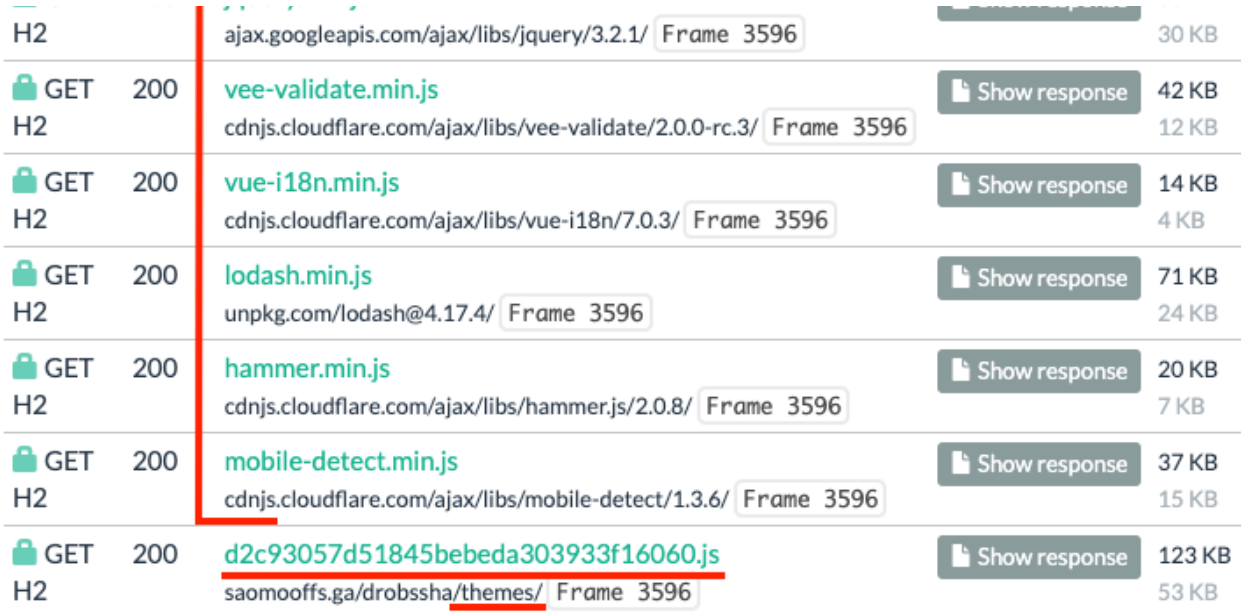


Figure 12: Transactions from First Known Sample

Additionally, it correlates strongly with the cluster of attack-related domains that were created just a couple of weeks earlier.

Question 2: How Widespread is this Attack?

After reviewing Group-IB's report, many of my thoughts around this topic had at least partial answers. I was, however, still unsure about what type of organizations were known to have been targeted in the last 18 months. To partially answer

This is a partial answer because my analysis is necessarily subject to several biases, most specifically Availability Bias.

this question, I focused on analyzing data from Urlscan to understand:

- how many known phishing portals existed, and where they were hosted
- which email addresses were entered by potential victims
- which Attack Vectors were used to deliver phishing lures

From this, I found that since May of 2020:
7403 total samples submitted

444unique phishing portals

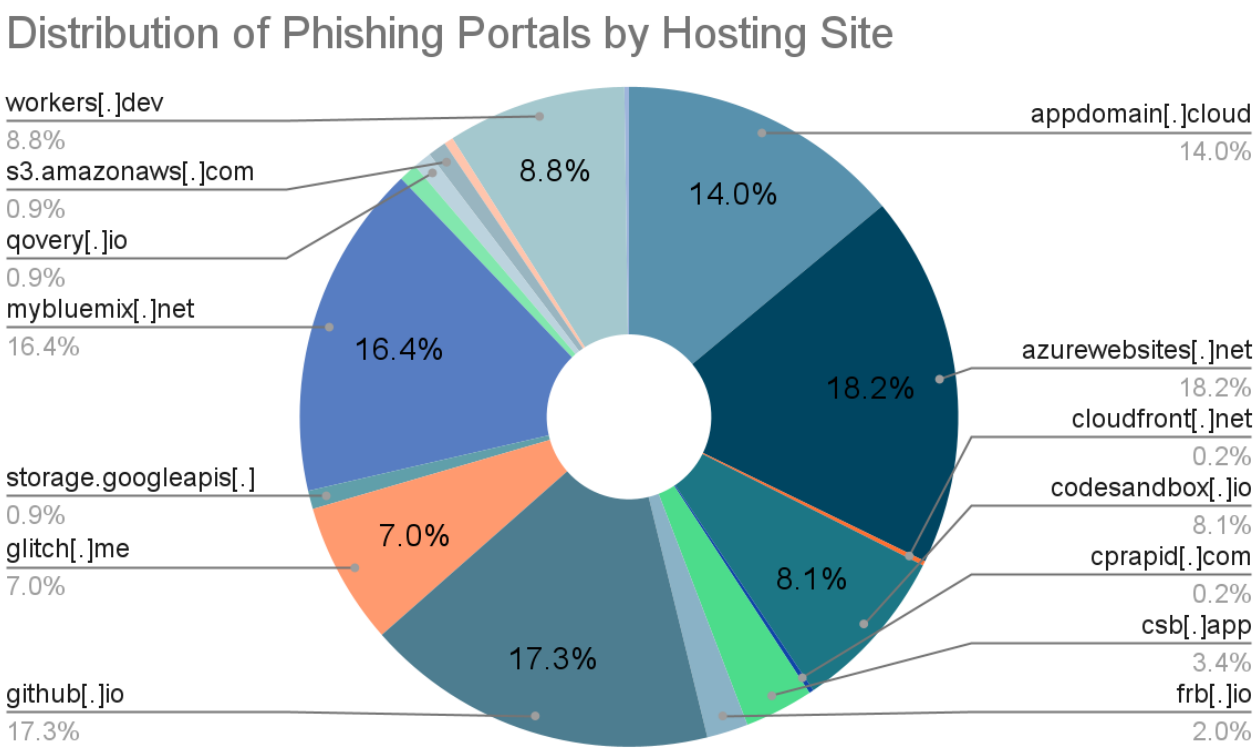


Figure 13: Distribution of Phishing Portals by Hosting Site

14 public or private sectors affected

Known Sectors Affected		
Government	Financial	Pharmaceutical
Energy	University	Insurance
Healthcare	Agriculture	Engineering
Aerospace	Public Relations	Legal
Technology	Marketing	

Realistically, because of the breadth and nature of this kit and the attacks, it's likely that virtually any industry could have been a target over time.

Kit Details

While the Group-IB report does a great job of covering many aspects of the kit, there are several items I'd like to elaborate on to help analysts understand when they have come across this activity in the wild.

Modular Infrastructure

This kit has two types of modularity. First, it makes deploying a phishing portal for many brands essentially drag-and-drop:

Figure 14: Template Locations for Various Portals in English and Vietnamese

There are eight templates supported out of the box. Interestingly, the choice to target some of these brands itself highlights the age of this phishing kit.While all of these templates are available, most known samples focus solely on Microsoft's Office365, with a small handful aiming to collect Outlook and other credentials. The second modular aspect of this kit is how the attack infrastructure itself is set up. While the particular customer of the kit controls some implementation decisions, there are four aspects for each campaign:

1. Front-End Phishing Portal (Short-Lived)

These sites are where the phishing portals load for a user. This is what a user would likely see in their browser when visiting a page. As an example:

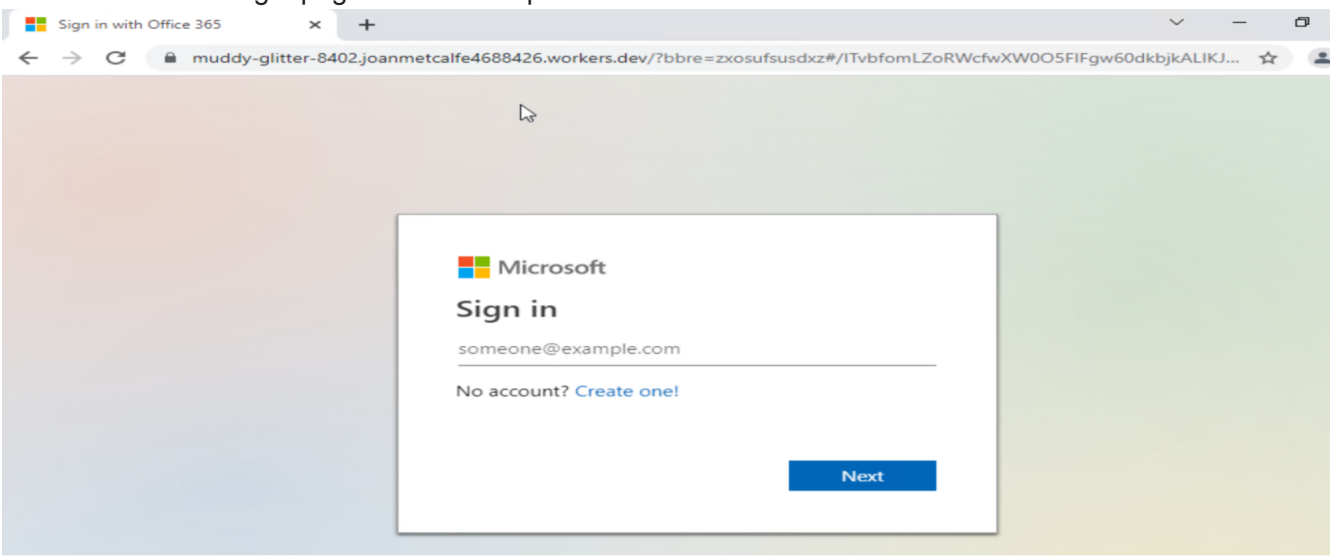


Figure 15: Example of a Front-End Phishing Portal

Because these are quickly detected and reported, they generally have a short shelf life.

2. Redirector Site (Long-Lived)

Redirector sites are lightweight, often Javascript-packed sites that are loaded by the phishing portal. Analysis of the unpacked code clearly indicates that their main duty is to request the appropriate template information and resources. In some samples (especially older ones), this site may be the same as the Template Hosting site. A screenshot of this code (unpacked) is reproduced below:

```
window.location.queryNBR = function getAllUrlParams(url) {
    var queryString = url ? url.split('?')[1] : window.location.search
        .slice(1);
    var obj = {};
    if (queryString) {
        queryString = queryString.split('#')[0];
        var arr = queryString.split('&');
        for (var i = 0; i < arr.length; i++) {
            var a = arr[i].split('=');
            var paramName = a[0];
            var paramValue = typeof(a[1]) === 'undefined' ? true : a[1];
            paramName = paramName.toLowerCase();
            if (typeof paramValue === 'string') paramValue = paramValue
                .toLowerCase();
            if (paramName.match(/\[(\d+)?\]$/)) {
                var key = paramName.replace(/\[(\d+)?\]/, '');
                if (!obj[key]) obj[key] = [];
                if (paramName.match(/\[\d+\]$/)) {
                    var index = /\[(\d+)\]/.exec(paramName)[1];
                    obj[key][index] = paramValue;
                } else {
                    obj[key].push(paramValue);
                }
            } else {
                if (!obj[paramName]) {
                    obj[paramName] = paramValue;
                } else if (obj[paramName] && typeof obj[paramName] ===
                    'string') {
                    obj[paramName] = [obj[paramName]];
                    obj[paramName].push(paramValue);
                } else {
                    obj[paramName].push(paramValue);
                }
            }
        }
    }
    return obj;
};

function loadScript(url, i) {
    var teat = i;
    if (i < 2) {
```

```
        var script = document.createElement("link");
        script.type = "text/css";
        script.rel = "stylesheet";
    } else {
        var script = document.createElement("script");
        script.type = "text/javascript";
    }
    if (script.readyState) {
        script.onreadystatechange = function() {
            if (script.readyState == "loaded" || script.readyState ==
                "complete") {
                script.onreadystatechange = null;
                i++;
                if (i < dml.length) {
                    loadScript(url, i);
                }
            }
        };
    } else {
        script.onload = function() {
            i++;
            if (i < dml.length) {
                loadScript(url, i);
            }
        };
    }
    if (i < 2) {
        script.href = url[teat];
    } else {
        script.src = url[teat];
    }
    document.getElementsByTagName("head")[0].appendChild(script);
};
var dml = [
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/css/b6fdd71dd75dbb30ce18df98c9e1efe0nbr1631036070.css",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/css/82e7a33a694e626e58725b38602a228anbr1631036070.css",
    "https://unpkg.com/axios@0.16.1/dist/axios.min.js",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/b6fdd71dd75dbb30ce18df98c9e1efe0nbr1631036070.js",
    "https://unpkg.com/vue@2.6.11/dist/vue.min.js",
    "https://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js",
    "https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js",
    "https://unpkg.com/lodash@4.17.4/lodash.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/b12687c7e1aebc71109c0493c0427e92.js"
];
if (('referrer' in document) && document.referrer == "") {
    if (!window.location.queryNBR().bbre) {
        document.getElementsByTagName("body")[0].innerHTML =
            "<div style='color:#222;
        text - align: unset;
        margin: 7 % auto 0;
        max - width: 390 px;
        min - height: 180 px;
        padding: 30 px 0 15 px;
        '><p><b>404.</b><ins style='
        color:
            #777;
                text-decoration:none;
                '>That's an error.</ins></p><p>The requested URL was not found on this server.<ins style= 'color:#777;
        text - decoration: none;
        '>That's all we know.</ins></p></div>";
        document.body.style.backgroundImage = "NONE";
        window.stop();
    } else loadScript(dml, 0);
} else loadScript(dml, 0);
```

Figure 16: Example of a Redirector Site's Code

Because it is generally less clear that these sites are malicious (unless one looks at a system that can correlate many samples), these generally stay active for many months. To give a concrete example, when working with the vendor where one of these sites was hosted, I was told that there was only **one unverifiable abuse report** filed in the many months that the site was active!

3. Template Hosting Site (Short-Lived)

The Template Hosting site hosts all of the Javascript, CSS, and sometimes image files used to render the phishing portal for the user. In some instances this site is the same as the Redirector site. The content is

always found in a subdirectory named `themes`:

```
var dml = [
    "https://walaptitizo.web.app/zbhjthsbzxvgzx/themes/css/cba05d9c5e08af626f068e5fc8f535acnbr1635176921.css",
    "https://walaptitizo.web.app/zbhjthsbzxvgzx/themes/css/7664a3ba333b09c811b4602594042a03nbr1635176921.css",
    "https://unpkg.com/axios@0.16.1/dist/axios.min.js",
    "https://walaptitizo.web.app/zbhjthsbzxvgzx/themes/cba05d9c5e08af626f068e5fc8f535acnbr1635176921.js",
"https://unpkg.com/vue@2.6.11/dist/vue.min.js",
"https://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js",
"https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js",
"https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js",
"https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js",
"https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js",
"https://unpkg.com/lodash@4.17.4/lodash.min.js",
"https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js",
    "https://walaptitizo.web.app/zbhjthsbzxvgzx/themes/c5cd8a00f456b35f83c4d3c71b56b90a.js"
];
```

Figure 17: Example of a Template Hosting Site Loading Assets

Because the Template Hosting sites are easy to pattern match against (which we'll discuss later) and view their resources, their shelf life is also short.

4. Credential Collection Site (Long-Lived)

The Credential Collection site is used to collect credentials that are entered by a user. These sites tend to stay up for extended periods of time (months or more) for a few reasons. First, they only appear when credential information has been entered, which does not occur in most sandbox environments. Second, all of the information is encrypted, which makes understanding the activity more difficult for most analysts. Third, they employ basic anti-analysis techniques that we'll describe in a moment.

Anti-Analysis Techniques

Outside of those discussed by Group-IB, there are two additional anti-analysis techniques employed by this phishing kit.

1. Code Packing

The Javascript code itself is obfuscated, as it is packed. Therefore, unpacking is required in order to look for any of the recognizable strings that exist within the code. Here is a before and after when using an

unpacker:

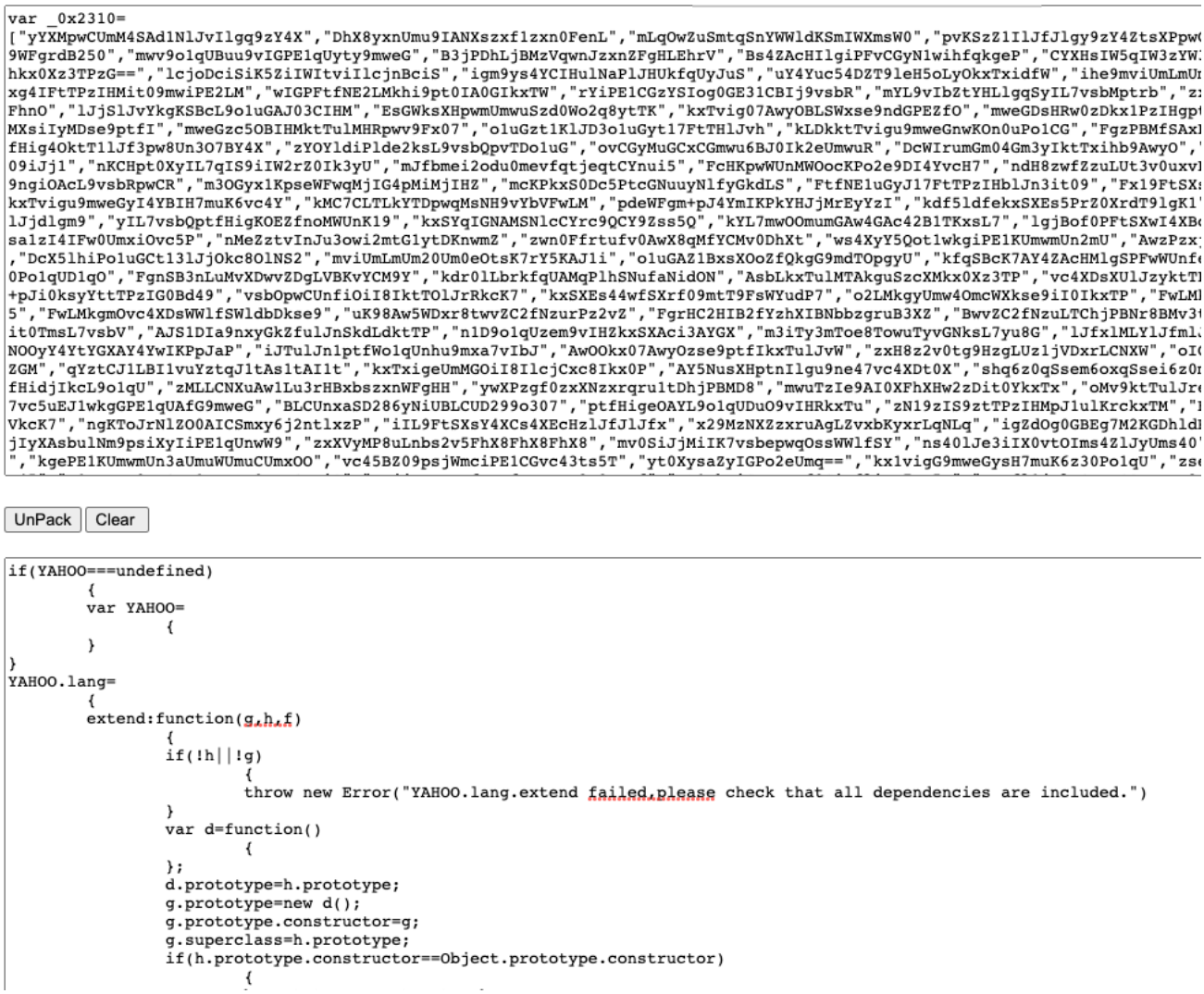


Figure 18: Before and After Code Unpacking

While this isn't something difficult to bypass, it does hinder the ability to look for exact string matches in the content.

2. Anti Chrome Dev Tools

Second, this kit has anti-debugging set up to block analysis by Chrome's Developer Tools. Any time Developer Tools is launched, the code triggers a `Pause` function:

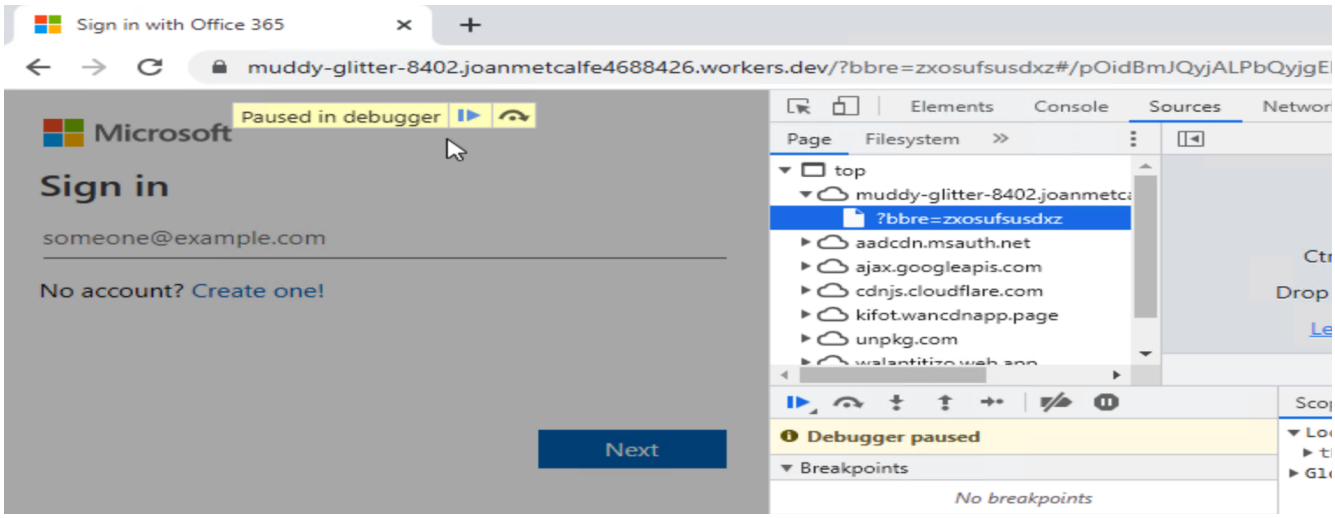


Figure 19: Anti-Debugging Found in Phishing Kit

This, combined with the fact that all communications are encoded and then encrypted, complicates analysis further. Fortunately, this can easily be bypassed by using an off-the-shelf proxy:

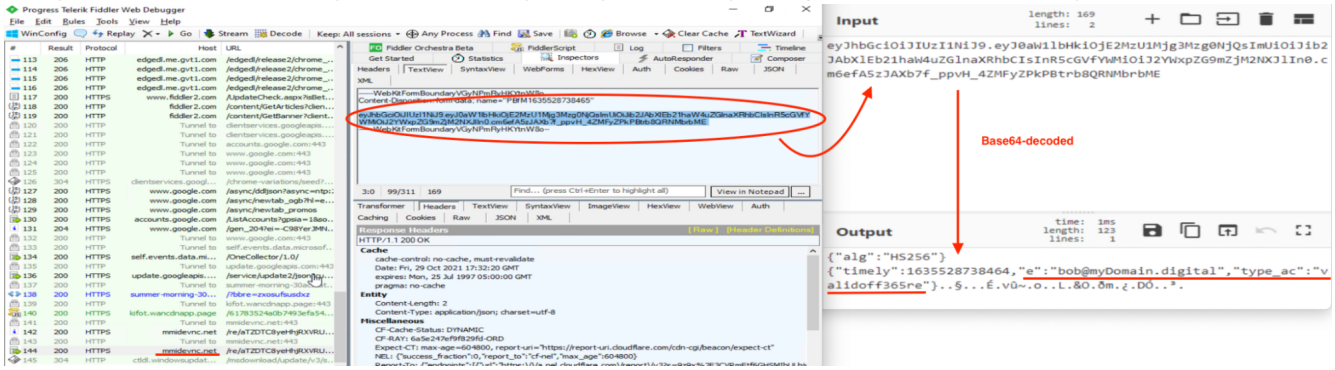


Figure 20: Decrypting and Decoding User-Submitted Payload in Fiddler and CyberChef

Attack Vectors

Concrete discussion about which vectors were used to deliver some malicious content at the beginning of an attack is something that rarely appears in threat intelligence reports. At SeclarityIO we believe that this is an underserved area that can be used to help all analysts understand tactics used repeatedly by adversaries. As we analyze more data going forward, we intend to eliminate this major blind spot. While we don't know everything that we'd like for this report, we do still know some things about which vectors were used to deliver the kit.At a high level, phishing is the #1 vector for delivery in this attack (as is true in a large majority of today's attacks). However, we also know that those phishing emails employed various techniques to hide their intent, and some amount of attacks originated outside of email. Since May 2020, the techniques we observed are as follows:

1. URL Shorteners

The use of URL shorteners can help to bypass some email protections, as well as add an air of legitimacy to a URL that disarms a suspicious user. The shorteners below were utilized.

URL Shorteners Observed			
bit[.]do	bit[.]ly	rb[.]gy	rebrand[.]ly
tiny[.]cc	tinyurl[.]com	u[.]to	cutt[.]ly

To see an example of what it looks like when a cutt[.]ly link is clicked and the user is redirected to a phishing portal, head to the How to Know If I'm Affected section.

2. Email Marketing Platforms

There were many samples which used `sendgrid[.]net` to bypass email filters and end up in users' inboxes.

3. Compromised Sites

Compromising sites is additional work for the adversary, but doing so provides them with the ability to hide more stealthily within an otherwise benign site. While we won't mention the sites that were compromised, there were several of them.

4. Malicious Domains

There were many domains set up by attackers with the intention to bypass security platforms by being unknown. The full list of known malicious domains can be found in the indicators section of this report.

5. Content Preview and Hosting Sites

Platforms that allow users to host arbitrary content on them are often used by attackers to quickly set up content and bypass security defenses. In addition to those platforms associated with the Phishing Portals, the following were observed:

Sites Observed		
gearhostpreview[.]com	fcert[.]co	googleusercontent[.]com

6. Advertisements

A few samples had redirects through Google's advertising infrastructure, specifically `googleads.g.doubleclick[.]net`

7. Open Redirects

It is possible to use certain sites in a malicious way without compromising them. One such example that appeared in the data set is `hangouts.google[.]com`

Open redirects ... and why Phishers love them. June 18, 2021. Accessible here.

.

Hunting and Detection

Since this phishing kit has been affecting thousands of organizations across more than four years, it is clear that there is not enough concrete information about how to successfully identify this activity across different layers of the security stack. In this section, I provide indicators that allow for security teams to not only identify what exists today ("specific indicators"), but also to identify the activity more broadly.

Specific Indicators

There are a wealth of specific indicators visible at various layers. These will be useful for detecting compromises that have already occurred, as well as those that do not adjust to the publishing of this report.
Note that as you review the indicators listed below, some of them have been **sampled** by analyzing one out of every 100 samples (across the total sample size of ~7400). This is because there is a massive number of sites and domains associated with this time period, and the value of many of these indicators has already expired (as the attack infrastructure evolves).

Known Front-End Phishing Portals by Hosting Platform (05/01/2020-11/04/2021)

Hosted on Microsoft's azurewebsites[.]net:

- http://cdoapponedripointa.azurewebsites[.]net
- http://itkoa92pixzda.azurewebsites[.]net
- http://rtodfxcidr9fdxciifd.azurewebsites[.]net
- http://xiaomtoedzxiucoda.azurewebsites[.]net
- https://abgotrgifxciiwresd.azurewebsites[.]net
- https://aereifzxooeret.azurewebsites[.]net
- https://anoappdevmodixzo.azurewebsites[.]net
- https://camemoae92paizxd.azurewebsites[.]net
- https://camori9apdsoxz.azurewebsites[.]net
- https://candeteappdemoaz.azurewebsites[.]net
- https://cdoapponedripointa.azurewebsites[.]net
- https://cmaorie9apxzodf.azurewebsites[.]net
- https://cmoas9pedixdga.azurewebsites[.]net
- https://cmoiae9xzdsoif.azurewebsites[.]net
- https://cniasauthosaizx.azurewebsites[.]net
- https://daglpcxoidrsd.azurewebsites[.]net
- https://detwyuitgnfcxxzas.azurewebsites[.]net
- https://digd0cxpodzxds.azurewebsites[.]net
- https://ertgoxicudsudyx.azurewebsites[.]net
- https://etqdlpodidfgerd.azurewebsites[.]net
- https://etrytuyiukhghfdd.azurewebsites[.]net
- https://ewetryhfdzd.azurewebsites[.]net
- https://ewirfozpxdsiifdfre.azurewebsites[.]net
- https://ewtryfglpxzxoda.azurewebsites[.]net
- https://gmatiaizxoisas.azurewebsites[.]net
- https://hkaoet9zxpdf.azurewebsites[.]net
- https://hkt0sdozxiidsx.azurewebsites[.]net
- https://ifd9osddisuxcdsdsf.azurewebsites[.]net
- https://itr9dxcouxc.azurewebsites[.]net
- https://kairmiizxoisa.azurewebsites[.]net
- https://kandeapmodepzox.azurewebsites[.]net
- https://kdantedmodeaptrial.azurewebsites[.]net
- https://khalyapdeowekozix.azurewebsites[.]net
- https://khkotaizixoxcuudsewr.azurewebsites[.]net
- https://kikadriveapps.azurewebsites[.]net
- https://kirwefdocxapsoxzifsd.azurewebsites[.]net
- https://las0pzxidsrfdcx.azurewebsites[.]net
- https://luxisoapdoeixz.azurewebsites[.]net

- https://mininaixzoaisde.azurewebsites[.]net
- https://minoapsostirotmos.azurewebsites[.]net
- https://mmodidiauzudszxias.azurewebsites[.]net
- https://mowebsoffisa039a.azurewebsites[.]net
- https://msairofif310doxz.azurewebsites[.]net
- https://odsigsdcpxivcdregf.azurewebsites[.]net
- https://otry0gfpcxidsdsx.azurewebsites[.]net
- https://ovdeiwsdzpzoidcx.azurewebsites[.]net
- https://oy0dpxzidfdvcxc.azurewebsites[.]net
- https://pt0dfxpcodsiiirdf.azurewebsites[.]net
- https://ptr0odfxciizds.azurewebsites[.]net
- https://qisamo0cxpdsf.azurewebsites[.]net
- https://rapatitiksharepmoreiz.azurewebsites[.]net
- https://retrytgfvlpdodfddf.azurewebsites[.]net
- https://retrytughfgxdsew.azurewebsites[.]net
- https://rot0dfxcpisdds.azurewebsites[.]net
- https://rtryflgpoidsfdxcfsd.azurewebsites[.]net
- https://rtrythlcvpxdsoretd.azurewebsites[.]net
- https://rtyuihjghfx.azurewebsites[.]net
- https://sae49rwsfczioda.azurewebsites[.]net
- https://sanjoffmoredoen.azurewebsites[.]net
- https://sdlroetigdxizusew.azurewebsites[.]net
- https://tairappdemmokiz.azurewebsites[.]net
- https://tgodvxpsorisfc.azurewebsites[.]net
- https://to9dfxpzi32s.azurewebsites[.]net
- https://toeq0dspxorwf.azurewebsites[.]net
- https://trp043edoosdfd.azurewebsites[.]net
- https://trytujygbcvxdsed.azurewebsites[.]net
- https://tyrodx0zppdscx.azurewebsites[.]net
- https://tyt65fgdfsdzxzds.azurewebsites[.]net
- https://uikjhgcxdsr.azurewebsites[.]net
- https://uyi87uhfcvxc.azurewebsites[.]net
- https://vaioriaedozciapxoz.azurewebsites[.]net
- https://vamoeoixnaosepdzx.azurewebsites[.]net
- https://vandapofisatopzox.azurewebsites[.]net
- https://vleworefdcpxzx.azurewebsites[.]net
- https://vmaoteidappzocidf.azurewebsites[.]net
- https://xcdseirfdocxpzxewesd.azurewebsites[.]net
- https://yogf9xc0zoisdsd.azurewebsites[.]net
- https://yto0dfxcozisads.azurewebsites[.]net

Hosted on Github's github[.]io:

- http://ad-wias.github[.]io
- http://af178zxtor.github[.]io
- http://agcasillasavalos.github[.]io
- http://aoid-doxi.github[.]io
- http://as-iwq.github[.]io
- http://bellasharp35.github[.]io

- http://blhughbanks.github[.]io
- http://bs29579.github[.]io
- http://carhenw43.github[.]io
- http://chris-gaowa.github[.]io
- http://conrad805.github[.]io
- http://cooperjame4et.github[.]io
- http://dansta3.github[.]io
- http://dbatchos.github[.]io
- http://dparked.github[.]io
- http://fultonmv.github[.]io
- http://ga-qisdizx.github[.]io
- http://jacobshamr91.github[.]io
- http://jasonvaughan2tr.github[.]io
- http://juanthomr0.github[.]io
- http://martoundav43re.github[.]io
- http://melert.github[.]io
- http://michelle-fong.github[.]io
- http://moskowba.github[.]io
- http://murrhanow2435fs.github[.]io
- http://nancysanm.github[.]io
- http://nigelrad.github[.]io
- http://plaughlinxz.github[.]io
- http://retirtigerapp.github[.]io
- http://roseramms0.github[.]io
- http://scottwagmr01.github[.]io
- http://seacoccs.github[.]io
- http://wendyturner8as.github[.]io
- http://wnumanga-neai.github[.]io
- https://af178zxtor.github[.]io
- https://aga-mrabel.github[.]io
- https://aiappdeoiz.github[.]io
- https://aldu201devs.github[.]io
- https://alea-eizx.github[.]io
- https://aro-ria.github[.]io
- https://asteinxz.github[.]io
- https://avea-owa.github[.]io
- https://aze-wiaa.github[.]io
- https://azx-xos.github[.]io
- https://bhughessv.github[.]io
- https://boa-owuzx.github[.]io
- https://chiria-asmppd.github[.]io
- https://ciw-aias.github[.]io
- https://connorhoward42.github[.]io
- https://daniellecham.github[.]io
- https://devida123.github[.]io
- https://directordallas.github[.]io
- https://dparked.github[.]io
- https://eric-sdixu.github[.]io

- https://fultonmv.github[.]io
- https://goodbaydeiz.github[.]io
- https://hbestasz.github[.]io
- https://honhadpap.github[.]io
- https://jhernandez19dev.github[.]io
- https://jkbeamon19.github[.]io
- https://koas-aoqiz.github[.]io
- https://lddimditi.github[.]io
- https://lysaghtzx.github[.]io
- https://managerkall.github[.]io
- https://moskowba.github[.]io
- https://neilwhite642.github[.]io
- https://nia-ozxi.github[.]io
- https://nwebster1zx.github[.]io
- https://ramiaalesdevgm200.github[.]io
- https://rogerwhem27.github[.]io
- https://sbartodviz.github[.]io
- https://terrilofad.github[.]io
- https://victoriacolmrs261.github[.]io
- https://wa-siai.github[.]io
- https://wendyturner8as.github[.]io
- https://wnumanga-neai.github[.]io

Hosted on IBM's mybluemix[.]net:

- https://alaotiadizucuxiczx-grumpy-ostrich-kp.mybluemix[.]net
- https://aoghisbjzkobzcijx.mybluemix[.]net
- https://bmoasmcxozovixz-generous-springhare-xl.mybluemix[.]net
- https://bngjhdgf-lean-wolverine-vb.mybluemix[.]net
- https://cbhj6fgxc-exhausted-bear.mybluemix[.]net
- https://cxogrifiizxocuvxc-funny-echidna-ql.eu-gb.mybluemix[.]net
- https://dvkosafixzosauu-responsive-hartebeest-wd.mybluemix[.]net
- https://ekiyhbuyzzydgbfxcb.mybluemix[.]net
- https://gamitiaozxiuaswq-noisy-hippopotamus-sc.mybluemix[.]net
- https://getstartednode-empathic-lizard-pq.mybluemix[.]net
- https://getstartednode-lean-wombat-sa.mybluemix[.]net
- https://ghgiuokjhgfdszx-accountable-reedbuck-xa.mybluemix[.]net
- https://h34fdxussouthcfappdomaincloud.mybluemix[.]net
- https://hammmairidevozx-kind-buffalo-rt.eu-gb.mybluemix[.]net
- https://hammzxoiufduxc-smart-badger-bb.mybluemix[.]net
- https://hgtuyiujghfgdfsd-boisterous-meerkat-py.eu-gb.mybluemix[.]net
- https://hgue43fdxc-unexpected-rabbit.mybluemix[.]net
- https://hkieadozxiiiczda-kind-dugong-qi.mybluemix[.]net
- https://itsociuxcoxzxdfd-patient-ostrich-ee.mybluemix[.]net
- https://jyjghfdcxzx-shiny-alligator-fp.mybluemix[.]net
- https://kaiynhapotirg8svizix-impressive-gecko-vd.mybluemix[.]net
- https://kamizibudigozox-happy-parrot-ve.mybluemix[.]net
- https://kgiaodzxxiuixzzx-wacky-zebra-ia.eu-gb.mybluemix[.]net
- https://kimapdcayturaz-restless-porcupine-vd.eu-gb.mybluemix[.]net

- https://kmizduscxuzxisds-surprised-tiger-hd.mybluemix[.]net
- https://koxzivjzx-proud-bandicoot-bo.mybluemix[.]net
- https://ksdoixuasdoxzizxi-comedic-quokka-kn.eu-gb.mybluemix[.]net
- https://ktiaoxzoxiifiozx-friendly-echidna-sm.mybluemix[.]net
- https://laitizxoisaudse-terrific-dugong-nm.mybluemix[.]net
- https://lakimditiitiaozix-turbulent-elephant-jv.mybluemix[.]net
- https://lieudzc9dcxiid-hilarious-cat-rb.mybluemix[.]net
- https://lpczviguficoxzisaf-exhausted-tiger-ni.mybluemix[.]net
- https://mamaapspotdev-patient-panther-ru.eu-gb.mybluemix[.]net
- https://mkodamodititiadoizx-wise-swan-aa.mybluemix[.]net
- https://mmgah9fzxoisaixz.mybluemix[.]net
- https://moamititaoszidizx-shiny-bandicoot-of.eu-gb.mybluemix[.]net
- https://moniiadzxoicuxcucx-silly-bushbuck-on.mybluemix[.]net
- https://motaot94wrosfciuzx.mybluemix[.]net
- https://ngaijuthaokivuznbm-empathic-chimpanzee-ks.mybluemix[.]net
- https://odsfiizxx-cheerful-llama-qb.mybluemix[.]net
- https://oeimaodiidzxxz-wise-mouse-wp.eu-gb.mybluemix[.]net
- https://otmaizxidsi-timely-panda-fi.mybluemix[.]net
- https://ovkzxijajzx-thankful-kudu-zm.mybluemix[.]net
- https://ozixsdcozx-surprised-lemur-us.eu-gb.mybluemix[.]net
- https://pandaoappoffertiraozx-thankful-gerenuk-my.eu-gb.mybluemix[.]net
- https://ramonappdix-wacky-numbat-mo.mybluemix[.]net
- https://riakvzoxvpougx-interested-oryx-kv.mybluemix[.]net
- https://rimavozxlagibucz.mybluemix[.]net
- https://sdg65gfxcxz-happy-impala.mybluemix[.]net
- https://sisahapdevgido-appreciative-grysbok-ax.mybluemix[.]net
- https://titikdaomizxisa-courteous-koala-ob.mybluemix[.]net
- https://ty5rtdfxc-fearless-chipmunk.mybluemix[.]net
- https://tyuyiyjghfgdxfc-shiny-swan-yw.mybluemix[.]net
- https://utaizxoxuxzusacxcx-daring-crocodile-wb.mybluemix[.]net
- https://uy76fgcv-turbulent-crocodile-pq.mybluemix[.]net
- https://vaingapapotiizxas.mybluemix[.]net
- https://vakgohkiynauzxvas-reliable-alligator-un.mybluemix[.]net
- https://vamdoahipzviiaxz-optimistic-swan-zj.mybluemix[.]net
- https://vanotoappzxoisdsd-courteous-raven-py.mybluemix[.]net
- https://vciirddf-intelligent-giraffe.mybluemix[.]net
- https://vcxb-sdjmndscx-courteous-lizard-gm.mybluemix[.]net
- https://vivamosgar0fspzis.mybluemix[.]net
- https://vlogritgdfzxiozx-balanced-gorilla-pv.mybluemix[.]net
- https://vmagiubozxviagaeq.mybluemix[.]net
- https://wamitieriu8dozxzx.mybluemix[.]net
- https://xzlaoihubzuxuaszxb-generous-porcupine-ru.mybluemix[.]net
- https://xzoiidsxzokcx-grumpy-giraffe-vf.mybluemix[.]net
- https://yt76yuhfgdx-impressive-fossa-wu.mybluemix[.]net
- https://yt86uyhfgd-nice-jaguar.mybluemix[.]net
- https://ytuyhjngbvcvxds-grumpy-numbat-dd.mybluemix[.]net
- https://zbhosknjifubjuzgszx-chatty-jaguar-hu.mybluemix[.]net
- https://zokvgif8bxcoozx.mybluemix[.]net

- https:/moniiadzxoicuxcucx-silly-bushbuck-on.mybluemix[.]net

Hosted on IBM's appdomain[.]cloud:

- http://mvaogidcxpziuixzoxzv-cheerful-ratel-kq.us-south.cf.appdomain[.]cloud
- https://akyihbzkoigizoovzbhs.us-south.cf.appdomain[.]cloud
- https://aoddimeiideudxz-delightful-eland-js.us-south.cf.appdomain[.]cloud
- https://awitiaoozxiiasx-happy-dingo-tn.eu-gb.cf.appdomain[.]cloud
- https://baodzkxzsa-boring-camel-wl.us-south.cf.appdomain[.]cloud
- https://bmaootygozxpoidaguz.us-south.cf.appdomain[.]cloud
- https://cagkosfispoz2xz.us-south.cf.appdomain[.]cloud
- https://cxnhkoyihuetfbzxysazxcczx.us-south.cf.appdomain[.]cloud
- https://dantianizxaisoap3iz.us-south.cf.appdomain[.]cloud
- https://ffmappadoaedz9dfd.us-south.cf.appdomain[.]cloud
- https://fkfaoirap9sdzoxzs.us-south.cf.appdomain[.]cloud
- https://g87ghbxcxs.us-south.cf.appdomain[.]cloud
- https://gamoaoorigjudiz32s.us-south.cf.appdomain[.]cloud
- https://ganmdomadievuxzx-excellent-kangaroo-am.us-south.cf.appdomain[.]cloud
- https://ghiaodzxokpzxosa-fantastic-rhinocerous-xt.us-south.cf.appdomain[.]cloud
- https://h34fdxussouthcfappdomaincloud.mybluemix.net
- https://ireutdfoxcxzuisx-patient-rhinocerous-da.us-south.cf.appdomain[.]cloud
- https://irmitmideivixzos-persistent-emu-oz.us-south.cf.appdomain[.]cloud
- https://kaigmyihsf9zpadsiczi.us-south.cf.appdomain[.]cloud
- https://laliak4ofxicizx.us-south.cf.appdomain[.]cloud
- https://liriaoxizuduuvxz-sleepy-ardvark-mp.eu-gb.cf.appdomain[.]cloud
- https://matguz9oxidsoxzsd.us-south.cf.appdomain[.]cloud
- https://mciaufanuxczozxusa-sweet-lizard-jc.us-south.cf.appdomain[.]cloud
- https://miamga9hrsfzoiusa.us-south.cf.appdomain[.]cloud
- https://mifaruadzpifizxc-exhausted-wombat-dr.eu-gb.cf.appdomain[.]cloud
- https://moamriaezxuxcizx.us-south.cf.appdomain[.]cloud
- https://nbiduaixzoxz-smart-gorilla-rw.us-south.cf.appdomain[.]cloud
- https://omcvisdcxz-chipper-koala-ed.us-south.cf.appdomain[.]cloud
- https://omiaizxoasiis-smart-roan-nv.eu-gb.cf.appdomain[.]cloud
- https://ovxziva-agile-serval-qp.us-south.cf.appdomain[.]cloud
- https://ozxisfdouzxusa-grateful-cat-au.us-south.cf.appdomain[.]cloud
- https://quairitideiizuxz-kind-bear-ty.us-south.cf.appdomain[.]cloud
- https://rakvoziusbfsozixuadxxz.us-south.cf.appdomain[.]cloud
- https://rhtr54d-boring-shark-jw.us-south.cf.appdomain[.]cloud
- https://ribzocpaodicd.us-south.cf.appdomain[.]cloud
- https://rimimozidievxz.us-south.cf.appdomain[.]cloud
- https://sandappmoz-optimistic-fox-lv.eu-gb.cf.appdomain[.]cloud
- https://santeidevmoapozx.eu-gb.cf.appdomain[.]cloud
- https://satlarigjha8sdozxi.us-south.cf.appdomain[.]cloud
- https://shrujikujghx-surprised-panda-kw.us-south.cf.appdomain[.]cloud
- https://temoatippdeizxi.us-south.cf.appdomain[.]cloud
- https://titkaiasozxa8sizx.us-south.cf.appdomain[.]cloud
- https://vakotiapptiauxzua.us-south.cf.appdomain[.]cloud
- https://vaqiw9zxozdoxzx.us-south.cf.appdomain[.]cloud
- https://vdzokkifdxcokzokx-nice-echidna-dx.us-south.cf.appdomain[.]cloud

- https://viakgasog9grfozix.us-south.cf.appdomain[.]cloud
- https://viapdevidoepa.eu-gb.cf.appdomain[.]cloud
- https://vkoziolzx-impressive-fossa-uy.us-south.cf.appdomain[.]cloud
- https://vmaiqegpaozxiad.us-south.cf.appdomain[.]cloud
- https://vmzigijvxcv-courteous-dingo-fc.us-south.cf.appdomain[.]cloud
- https://vndfzvfasf-funny-jackal-hb.us-south.cf.appdomain[.]cloud
- https://xcfd54dcx-delightful-wallaby-gv.us-south.cf.appdomain[.]cloud
- https://xchsdghd-grouchy-ostrich-sz.us-south.cf.appdomain[.]cloud
- https://xinviaoafinabatizx.us-south.cf.appdomain[.]cloud
- https://xmanomoemeizxoas-quick-ostrich-ol.us-south.cf.appdomain[.]cloud
- https://xnbsdg-intelligent-badger-xk.us-south.cf.appdomain[.]cloud
- https://xnxcbsd-restless-lizard-kh.us-south.cf.appdomain[.]cloud
- https://zbksogsokdzxkouzxc-daring-koala-pv.eu-gb.cf.appdomain[.]cloud
- https://zkahibolaoideunslie-xicuf.us-south.cf.appdomain[.]cloud
- https://zoigdizxkvoaokvxz.us-south.cf.appdomain[.]cloud
- https://zvbhsjkyrjdtfxbcgda.us-south.cf.appdomain[.]cloud
- https://zvkohsugdifzobiuzgad.us-south.cf.appdomain[.]cloud

Hosted on Cloudflare's workers[.]dev:

- http://black-sunset-d9cd.kinlee-f9.workers[.]dev
- http://cold-meadow-ed58.edgarsutto-n-6286-2-0-4.workers[.]dev
- http://cold-violet-a946.dorismar.workers[.]dev
- http://gentle-star-48a5.jerry-bakermr2391988.workers[.]dev
- http://icy-band-02ec.hassel.workers[.]dev
- http://jollysratgzozi8dixzo.shamekia.workers[.]dev
- http://lingering-disk-aabf.jawana85.workers[.]dev
- http://purple-field-a89f.garlon0.workers[.]dev
- http://raspy-sun-8415.lesieli7.workers[.]dev
- http://shiny-bread-6d2a.tiny120.workers[.]dev
- http://spring-math-e458.aahil40.workers[.]dev
- http://tiny-fog-dd5c.m-goetz.workers[.]dev
- http://wild-bush-7b61.shella05.workers[.]dev
- http://winter-surf-59e1.springbud.workers[.]dev
- http://wispy-shadow-7ff9.graig.workers[.]dev
- https://billowing-violet-6f58.london78.workers[.]dev
- https://black-cloud-085f.hanson-banner.workers[.]dev
- https://blue-heart-e06c.silva849.workers[.]dev
- https://broad-wildflower-a967.michelle7333.workers[.]dev
- https://dawn-bonus-f123.carma17.workers[.]dev
- https://dry-rice-cb7d.kenneth451.workers[.]dev
- https://empty-haze-faa2.kodi4863.workers[.]dev
- https://falling-salad-d49a.saragonzales5348.workers[.]dev
- https://fancy-moon-248a.ahniah7.workers[.]dev
- https://flat-resonance-1730.akeria54.workers[.]dev
- https://flat-wind-bdd3.rachelannef15.workers[.]dev
- https://gentle-field-0465.keshawn-9.workers[.]dev
- https://gentle-firefly-4ff9.teranf76.workers[.]dev
- https://gentle-king-59b9.aleanna9.workers[.]dev

- https://gentle-star-48a5.jerry-bakermr2391988.workers[.]dev
- https://lingering-base-e6b9.mmulkerrin.workers[.]dev
- https://lingering-mountain-0923.deron-seraphim.workers[.]dev
- https://nameless-heart-fc3a.dior9129.workers[.]dev
- https://orange-recipe-b20c.salma68.workers[.]dev
- https://purple-disk-7db5.quetzaly.workers[.]dev
- https://still-art-c252.twana.workers[.]dev
- https://sweet-block-a4c5.mmulkerrin.workers[.]dev
- https://vivjagmoktuxzoas.kazandra.workers[.]dev
- https://wild-waterfall-e7b2.norwood7618.workers[.]dev

Hosted on CodeSandbox's codesandbox[.]io:

- http://1yxk7.codesandbox[.]io
- http://2dnq2.codesandbox[.]io
- http://2ghm7.codesandbox[.]io
- http://815ox.codesandbox[.]io
- http://cqu62.codesandbox[.]io
- http://epq7u.codesandbox[.]io
- http://ew4u2.codesandbox[.]io
- http://g94wu.codesandbox[.]io
- http://lkwkj.codesandbox[.]io
- http://pk33o.codesandbox[.]io
- http://qr3xp.codesandbox[.]io
- http://sy7fh.codesandbox[.]io
- http://tw59l.codesandbox[.]io
- http://ws7xo.codesandbox[.]io
- http://yh4yj.codesandbox[.]io
- https://11854.codesandbox[.]io
- https://1dil9.codesandbox[.]io
- https://1g6qj.sse.codesandbox[.]io
- https://2dnq2.codesandbox[.]io
- https://2ghm7.codesandbox[.]io
- https://402hd.codesandbox[.]io
- https://44zfi.codesandbox[.]io
- https://815ox.codesandbox[.]io
- https://8rdoh.codesandbox[.]io
- https://cqu62.codesandbox[.]io
- https://dciwl.codesandbox[.]io
- https://ew4u2.codesandbox[.]io
- https://glwn0.codesandbox[.]io
- https://jnjor.codesandbox[.]io
- https://jrb4i.codesandbox[.]io
- https://mxjek.sse.codesandbox[.]io
- https://pcpqg.codesandbox[.]io
- https://sy7fh.codesandbox[.]io
- https://vg147.codesandbox[.]io
- https://vip6y.codesandbox[.]io
- https:/jrb4i.codesandbox[.]io

Hosted on Glitch's glitch[.]me:

- https://aback-supreme-colby.glitch[.]me
- https://abrupt-flannel-devourer.glitch[.]me
- https://adventurous-jewel-othnielia.glitch[.]me
- https://alluring-feline-web.glitch[.]me
- https://assorted-slash-marmoset.glitch[.]me
- https://band-quaint-saguaro.glitch[.]me
- https://calm-copper-course.glitch[.]me
- https://cautious-thread-hyena.glitch[.]me
- https://decisive-sleepy-antlion.glitch[.]me
- https://fog-numerous-fine.glitch[.]me
- https://hospitable-airy-walk.glitch[.]me
- https://invincible-soapy-spectacles.glitch[.]me
- https://iris-handy-newt.glitch[.]me
- https://knowing-numerous-cloud.glitch[.]me
- https://linen-bead-summer.glitch[.]me
- https://lizard-level-windshield.glitch[.]me
- https://lopsided-time-afrovenator.glitch[.]me
- https://majestic-magic-sunday.glitch[.]me
- https://mixolydian-wandering-shamrock.glitch[.]me
- https://night-noon-bedbug.glitch[.]me
- https://oil-alpine-pancreas.glitch[.]me
- https://petite-spotty-echo.glitch[.]me
- https://quill-puzzling-custard.glitch[.]me
- https://rattle-marred-pamphlet.glitch[.]me
- https://respected-carnelian-judge.glitch[.]me
- https://scientific-elderly-earthquake.glitch[.]me
- https://south-rift-april.glitch[.]me
- https://spectrum-delirious-tailor.glitch[.]me
- https://tabby-tropical-utahraptor.glitch[.]me
- https://tall-friendly-rover.glitch[.]me
- https://valley-puddle-currency.glitch[.]me

Hosted on CodeSandbox's csb[.]app:

- http://ejdxf.csb[.]app
- http://ohfhj.csb[.]app
- http://pq4ig.csb[.]app
- http://tp0rs.csb[.]app
- https://6b46l.csb[.]app
- https://bepyh.csb[.]app
- https://ibreg.csb[.]app
- https://ijh43.csb[.]app
- https://kfku5.csb[.]app
- https://lj1rf.csb[.]app
- https://pqsil.csb[.]app
- https://txwex.csb[.]app
- https://uhkqg.csb[.]app

Hosted on fortrabbit's frb[.]io:

- https://camomimlikeaposi.frb[.]io
- https://custom-hpbm.frb[.]io
- https://czxioaperfdicx.frb[.]io
- https://niapdititademoz.frb[.]io
- https://riaiga9gapdogia.frb[.]io
- https://sanihdviosapxz.frb[.]io
- https://vaoepdpirieodsds.frb[.]io
- https://viapeteiadxcopds.frb[.]io
- https://viapreilsdirsd.frb[.]io

Hosted on Amazon's s3.amazonaws[.]com:

- https://aamkagu0nguwm2fklwi4mgutndc3my1izwqxltnjowzmnzyznjdkzgbgaaaaaab.s3.amazonaws[.]com
- https://nwrsdzd.s3.amazonaws[.]com
- https://sdkopzxo.s3.amazonaws[.]com
- https://tadozida.s3.amazonaws[.]com

Hosted on Google's storage.googleapis[.]com:

- https://storage.googleapis.com/allabaonsha.appspot[.]com
- https://storage.googleapis.com/cfar0apoxz.appspot[.]com
- https://storage.googleapis.com/cfar0apoxz.appspot[.]com
- https://storage.googleapis.com/staging.cgf6uyhfs.appspot[.]com

Hosted on Qovery's qovery[.]io:

- http://main-watappx-dm2juipiptfiui5r-gtw.qovery[.]io
- https://main-simple--zh43qyrso3e4llzo-gtw.qovery[.]io
- https://main-tamalzm-pkwi8p288p2p7fkd-gtw.qovery[.]io
- https://main-vana1-vpou9j59zrnysrxi-gtw.qovery[.]io

Hosted on Cloudfront's cloudfront[.]net:

https://d3cb5gpmkas4zk.cloudfront[.]net

Hosted on cPanel's cprapid[.]com:

https://www.176-119-1-189.cprapid[.]com

Sampling of Known Redirector Sites (05/01/2020-11/04/2021)

Site Name	Last Seen
*.wancdnapp[.]page	11/09/2021 This site went undetected for 8 months until we worked with a vendor to block it.

*.aioecoin[.]org	09/05/2021
*.smsmail[.]net	07/31/2021
*.perfectstuff[.]info	01/26/2021
ameizoxposaewe.herokuapp[.]com	11/17/2020

Sampling of Known Template Hosting Sites (05/01/2020-11/04/2021)

- wianziasocnds.web[.]app
- vgrelaxacndapp.web[.]app
- walaptitizo.web[.]app
- rikapcndbn.web[.]app
- conroaioxzfrecnd.herokuapp[.]com
- vmiaappfcndfreis.herokuapp[.]com
- uy7rsdxs.web[.]app
- bboxc98sz.web[.]app
- as9wepsdxo.web[.]app
- as9wepsdxo.firebaseapp[.]com
- cvbv54fsaz.web[.]app
- yu76dfxxz.web[.]app
- wrty65tfzx.web[.]app
- vcg5gvxc.web[.]app
- appdemotrailtes.firebaseapp[.]com
- vcbn65fgxzx.firebaseapp[.]com
- aptsonewcndapp.web[.]app
- lapcndfrehaopzx.firebaseapp[.]com
- viapceaotiadzx.web[.]app
- nealpncdapp.firebaseapp[.]com
- vancndnewis.web[.]app
- vkrisfoia.web[.]app
- vipcndvvappdev.web[.]app
- vapdelbnbapp.web[.]app
- sandanappdmocnd.firebaseapp[.]com
- cndappcontentims.web[.]app
- crdnclimitappdemo.firebaseapp[.]com
- gadancdappdtriapz.web[.]app
- miacndapmamaslpot.firebaseapp[.]com
- atnkamcndtepa.firebaseapp[.]com
- mamodmiappscn.web[.]app
- kamppcnddemoiz.web[.]app
- nirsonappx.firebaseapp[.]com
- vankakaapdmeo.firebaseapp[.]com
- snamomidcndsx.web[.]app
- kamppcnddemoiz.web[.]app
- nanijsappdncs.web[.]app
- karikappdemo.firebaseapp[.]com
- manaapdpemtri.firebaseapp[.]com
- gapptitikzxi.firebaseapp[.]com

Known Credential Collection Sites (05/01/2020-11/04/2021)

- mmidevnc[.]net
- bugcart[.]com
- bestnewsworld[.]info
- thenewshot[.]com
- c3y5-tools[.]com

Known Malicious Domains (05/01/2020-11/04/2021)

- lcregruop[.]com
- nyembroideystudio[.]com
- aitfax[.]com
- aosfax[.]com
- asdfax[.]com
- efaxx[.]org
- auefax[.]com
- avsfax[.]com
- awsfax[.]com
- e-faxx[.]online
- efaxx[.]online
- auntyeinstein[.]com
- cascadesociety[.]in
- corporacioncela[.]com
- emryspartners[.]com
- made4love[.]co[.]uk
- remit-confirmation[.]com
- rfq-document[.]com
- confirmation-document[.]page
- bestshorttermloan[.]com
- skyhighgardensupplies[.]com
- tkdesigns-eg[.]com
- alturawlqcs[.]com
- bio-se7ati[.]com
- combresstec[.]gq
- crummycare[.]com
- insuriogroup[.]info
- pvhnk.app[.]link
- www.billings-notificati[.]com
- mypayrollupdate[.]com
- www.online-confirmation[.]page
- tfarmer.aa1ghhjnhyhj[.]com
- themoyacompanies[.]com
- viacomcbs-france[.]com

6. Recaptcha Key

Inside the core phishing kit code that is repackaged and identical for the last 4+ years, there is a reference to the kit's Google Recaptcha site key:

```
13940     methods: {
13941         renderC: function() {
13942             if (this.readyGCaptcha && !this.recaptcha) {
13943                 var me = this;
13944                 var momo = function() {
13945                     if (window.grecaptcha) {
13946                         var res = grecaptcha.getResponse(me.recaptcha);
13947                         if (res == "" || res == undefined || res.length == 0) {
13948                             me.valueres = "";
13949                         } else me.valueres = res;
13950                     }
13951                 };
13952                 var excb = function() {
13953                     me.valueres = "";
13954                 };
13955                 this.checkLoadRecaptcha = false;
13956                 this.recaptcha = grecaptcha.render(document.getElementById(this.idcaptcha), {
13957                     'sitekey': '6Lc_yyYUAAAAAJYQzVrpY-6ylYLSfpcaKbPJGyJP',
13958                     'theme': 'light',
13959                     'callback': momo,
13960                     'expired-callback': excb
```

Figure 21: Recaptcha Key in Beautified Code

Checking in with Google on this, I learned that this was in fact able to help identify a significant number of sites.

7. Strings and Regexes

If you have the ability to inspect URLs and file contents, there are many useful things that can help to identify this phishing kit. In all samples, the Javascript and CSS files used to set up and render the phishing portal can be found as such:

`/\/themes\/(((js|css)\/)|)[a-zA-Z0-9]45\.(js|css)/`

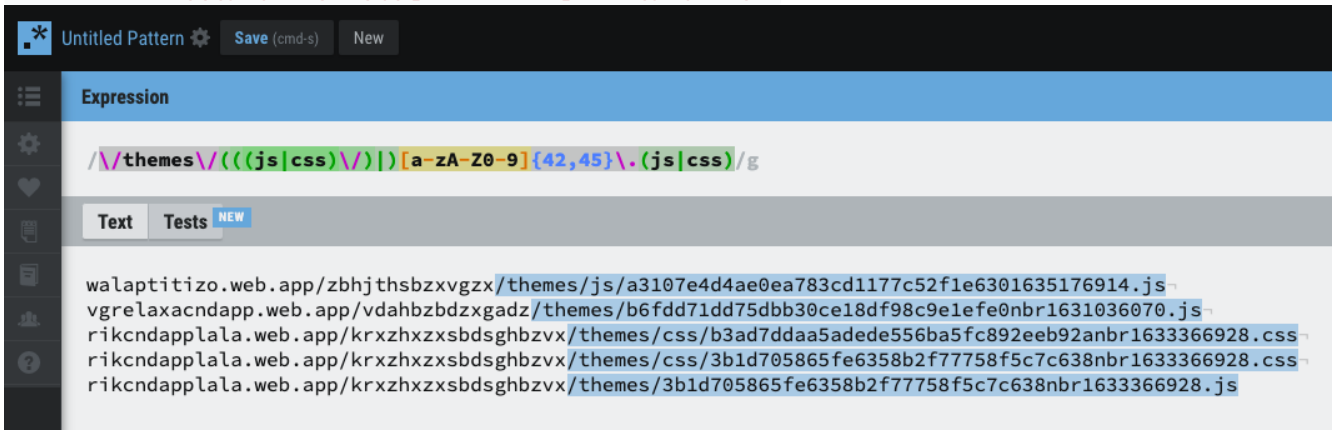


Figure 22: Regex in Action

Moreover, the string `nbr` is repeated constantly in the phishing kit's files and in some of the URLs used to request Javascript and CSS content (as seen above).

Broad Indicators

Broad indicators allow this activity to continue to be detected while the underlying phishing kit remains the same, even as the infrastructure itself evolves. Because this kit is used by many criminal groups and has remained static for over four years, it is likely that these indicators will remain useful long-term.

1. Open-Source Libraries Loading

In every instance of this phishing kit's use, there are a handful of libraries requested in order. This can be seen (after unpacking and beautifying) in the following code:

```
var dml = [
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/css/b6fdd71dd75dbb30ce18df98c9e1efe0nbr1631036070.css",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/css/82e7a33a694e626e58725b38602a228anbr1631036070.css",
    "https://unpkg.com/axios@0.16.1/dist/axios.min.js",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/b6fdd71dd75dbb30ce18df98c9e1efe0nbr1631036070.js",
    "https://unpkg.com/vue@2.6.11/dist/vue.min.js",
    "https://unpkg.com/vue-router@2.7.0/dist/vue-router.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vuex/2.3.1/vuex.min.js",
    "https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vee-validate/2.0.0-rc.3/vee-validate.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/vue-i18n/7.0.3/vue-i18n.min.js",
    "https://unpkg.com/lodash@4.17.4/lodash.min.js",
    "https://cdnjs.cloudflare.com/ajax/libs/mobile-detect/1.3.6/mobile-detect.min.js",
    "https://vgrelaxacndapp.web.app/vdahbzbdzxgadz/themes/b12687c7e1aebc71109c0493c0427e92.js"
```

Figure 23: Block of Code Loading Open Source Libraries

Comparing the first-known sample with one from recent days, we see this behavior matching identically:

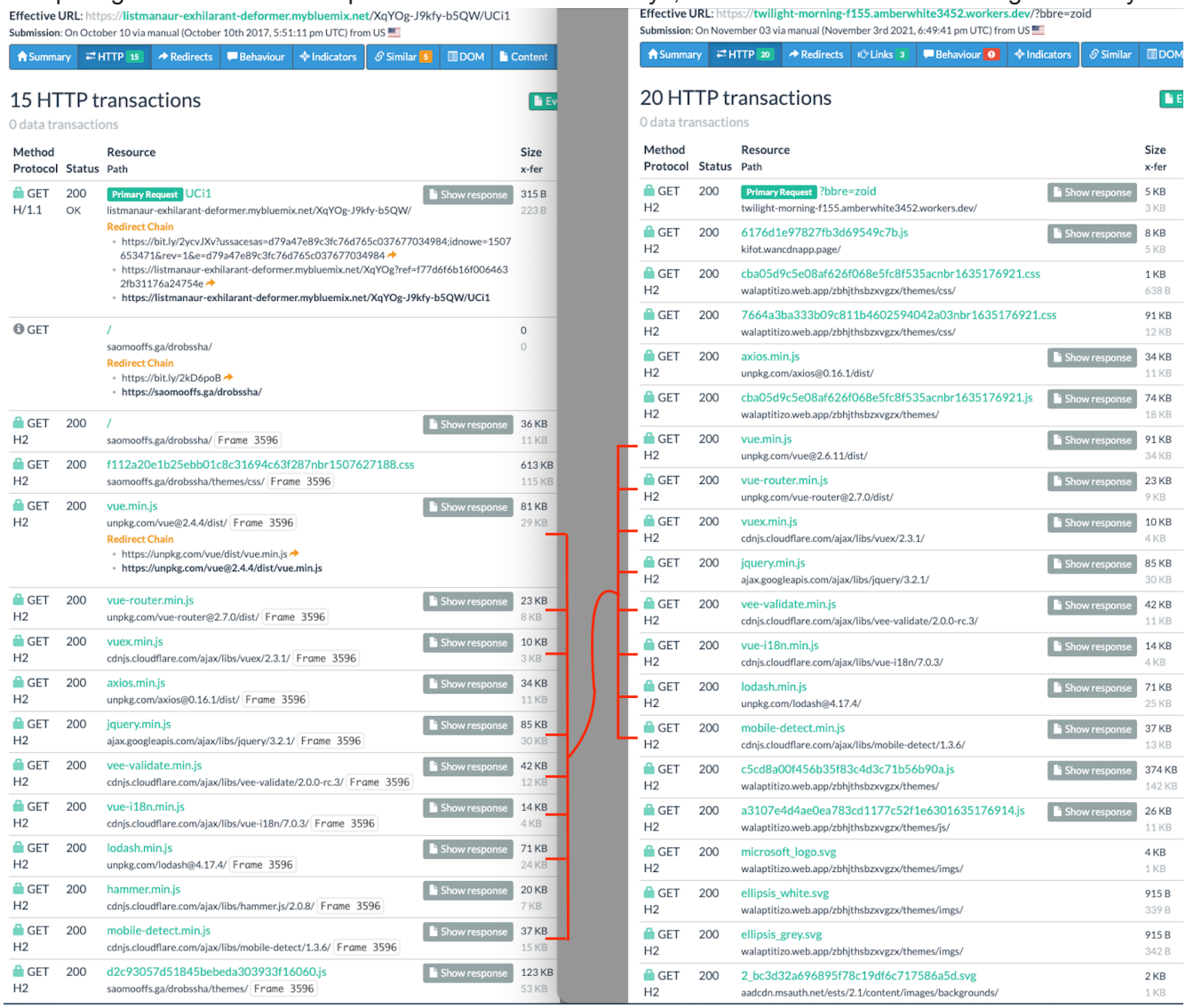


Figure 24: Open Source Libraries Load Identically Over Time

If you have access to a decrypted version of the information you can match things exactly as seen above. However, it's also possible to identify this activity on the network! Below we see how an example of this activity appears in NetworkSage. Multiple requests to the same CDN are grouped together into one

encrypted session, which provides a more succinct view:

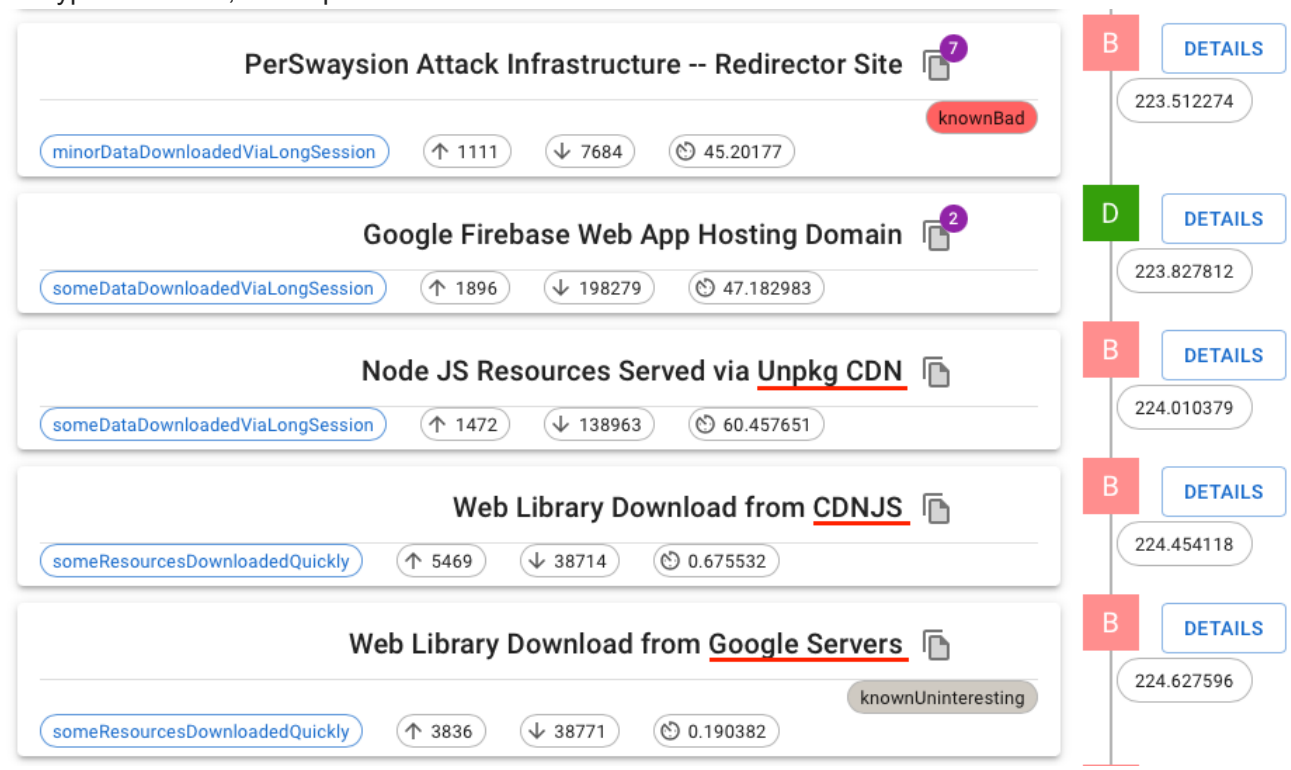


Figure 25: Network View of Open Source Libraries Loading

2. Content Loading from Cloud Hosting Platforms

The second indicator for these (and for a wider range of) attacks is understanding how common some cloud hosting site is. Since these sites are acting as nearly one-use phishing portals in this activity, it's likely that you'll see that they are incredibly uncommon across the global population:

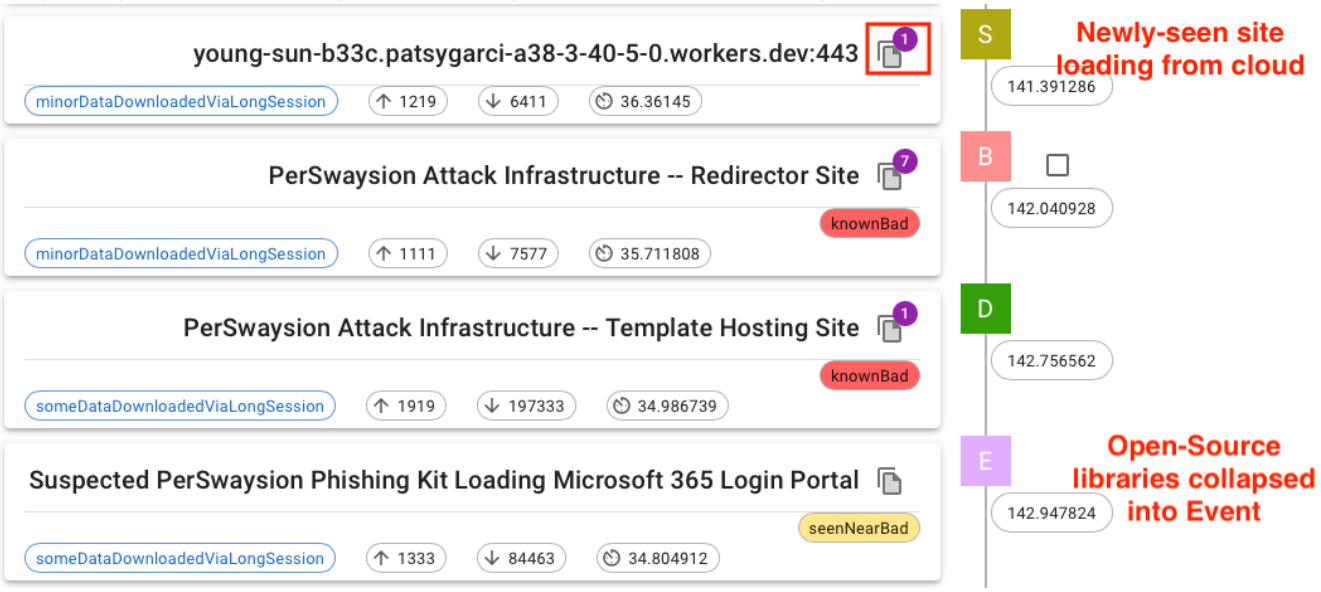


Figure 26: Uncommon Cloud-Hosted Activity

Other Notes

How to Know if I'm Affected

Knowing how far the phishing attack got -- as well as how it arrived for your users -- can be learned by analyzing the network traffic around the activity. For example, if your users were targeted by an attack that arrived via phishing through your Microsoft 365 instance, you'll likely see activity like the following:

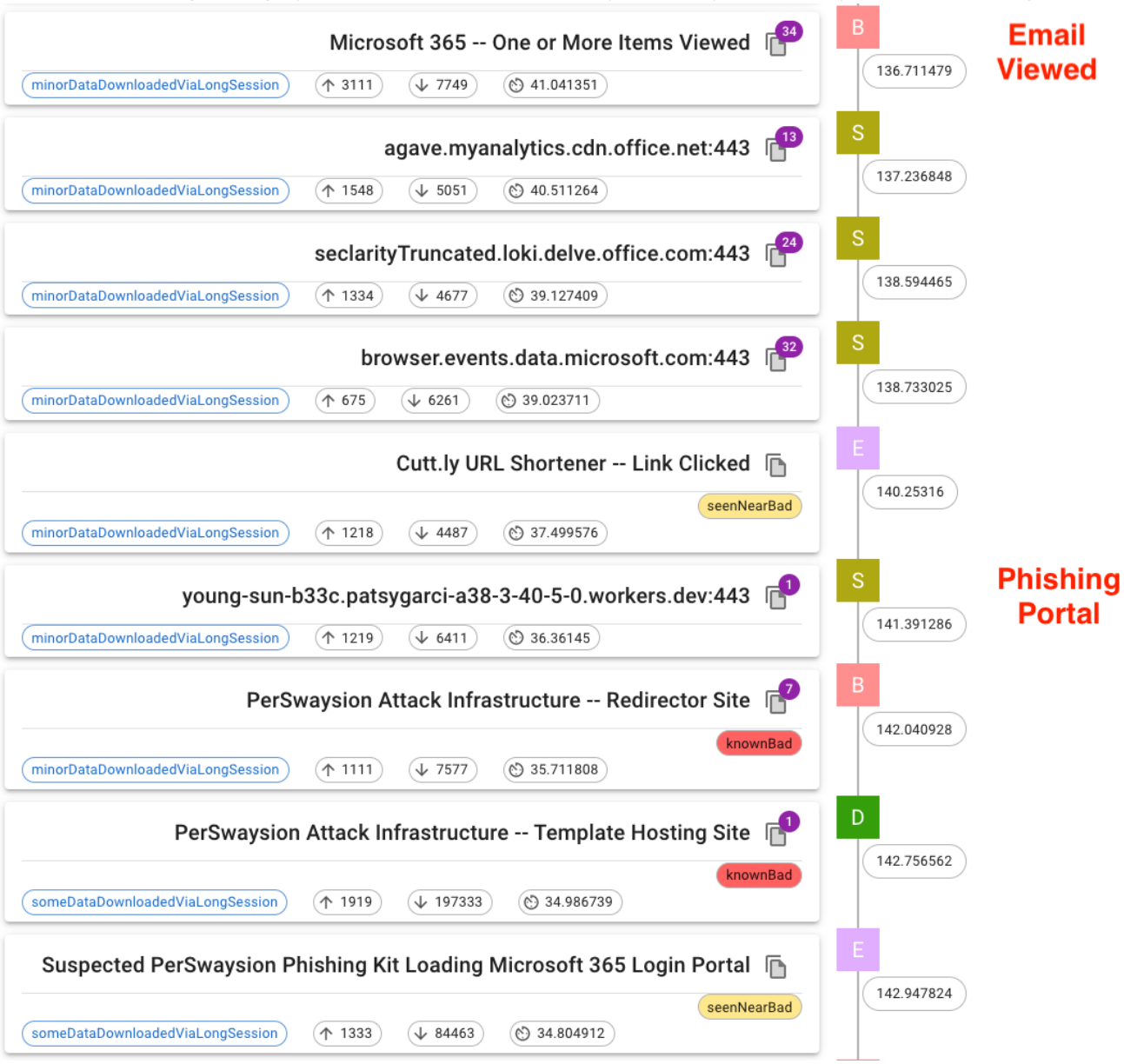


Figure 27: User Clicked on Email Containing cutt[.]ly Link for Phishing Portal

In the case above, we also discover that the user very likely received an email where the malicious domain was hidden behind a Cuttly URL shortening link, one of many URL shorteners that have been used to deliver malicious links in this and various other phishing attacks. To learn if your users have entered credentials, there are two things to look for. First, you should be on the lookout for recent known Credential Collection sites. These are automatically labeled and described for your convenience in NetworkSage:

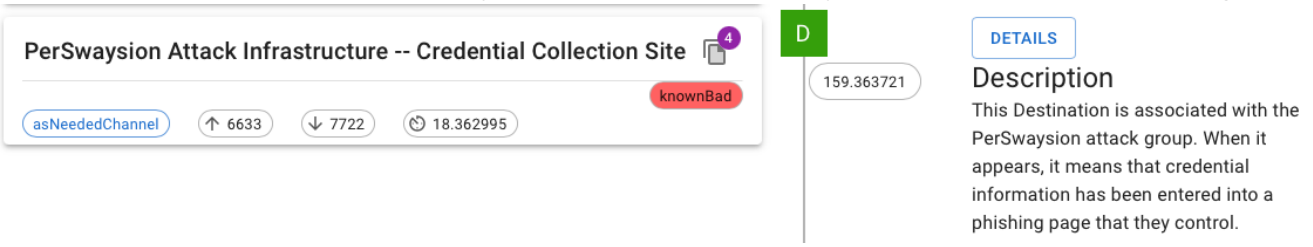


Figure 28: Labeled Credential Collection Site

Second, if the site is not yet recognized, be on the lookout for uncommonly-occurring activity that suggests a C2-like channel is set up soon after other indicators of this attack:

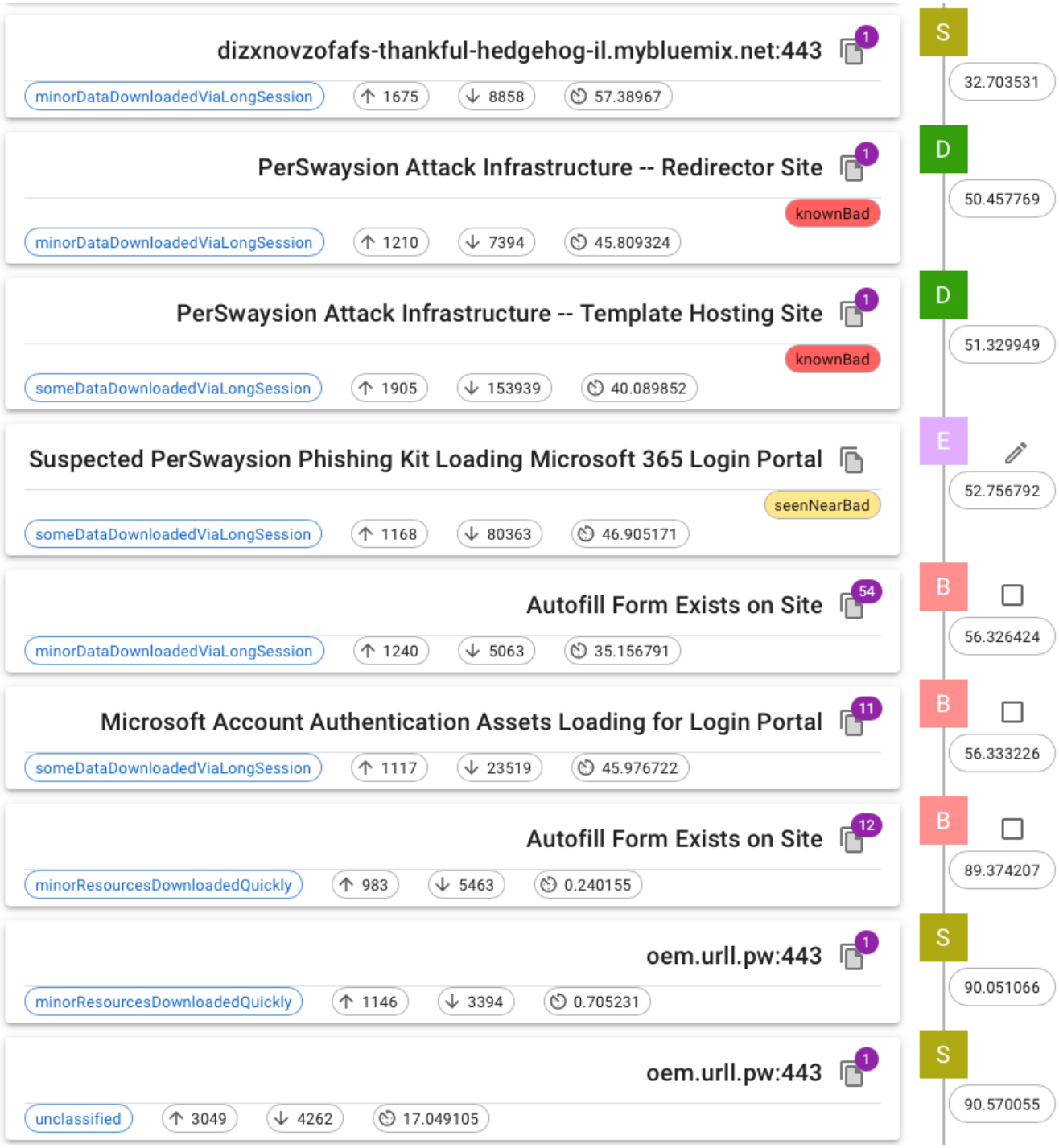


Figure 29: Site with C2-like Behavior Near Known PerSwaysion Indicators

If you submit your samples to NetworkSage and don't see any indication of the C2 activity above, it's likely that the user decided to leave the site before entering any information.

Loose Ends

There are several loose ends that I've come across in the investigation of this phishing kit that I'd like to share with the community in hopes that it helps to continue crippling this infrastructure and the group behind the kit.

1. How is this kit marketed?

I am far from an expert on Dark Web activity, but my searching on various forums turned up no meaningful leads. Moreover, none of the strings (outside of those that I've mentioned) in any of the files I've analyzed have appeared anywhere on the Internet.

2. Who developed this kit?

Group-IB's report identified that the developers likely spoke Vietnamese natively, but no other ties to the developers themselves were mentioned (there were references to users who bought the platform, but that isn't what I'm interested in). Despite extensively searching a couple of possible leads associated with Vietnamese developers, my search turned up nothing fruitful.

3. What was the anytools[.]biz site?

While I found references to anytools[.]biz app development in many samples that existed from 2019 onward, I was unable to find any historical information (including via the Internet Archive) about this site or its contents.

4. Is this a view of an early UI?

While analyzing one site that served as a Credential Collection site in mid-2019 (`dtvd[.]biz`), I noticed that one of the samples that appeared in Urlscan had a page that referenced a Gmail Auto Login GUI:

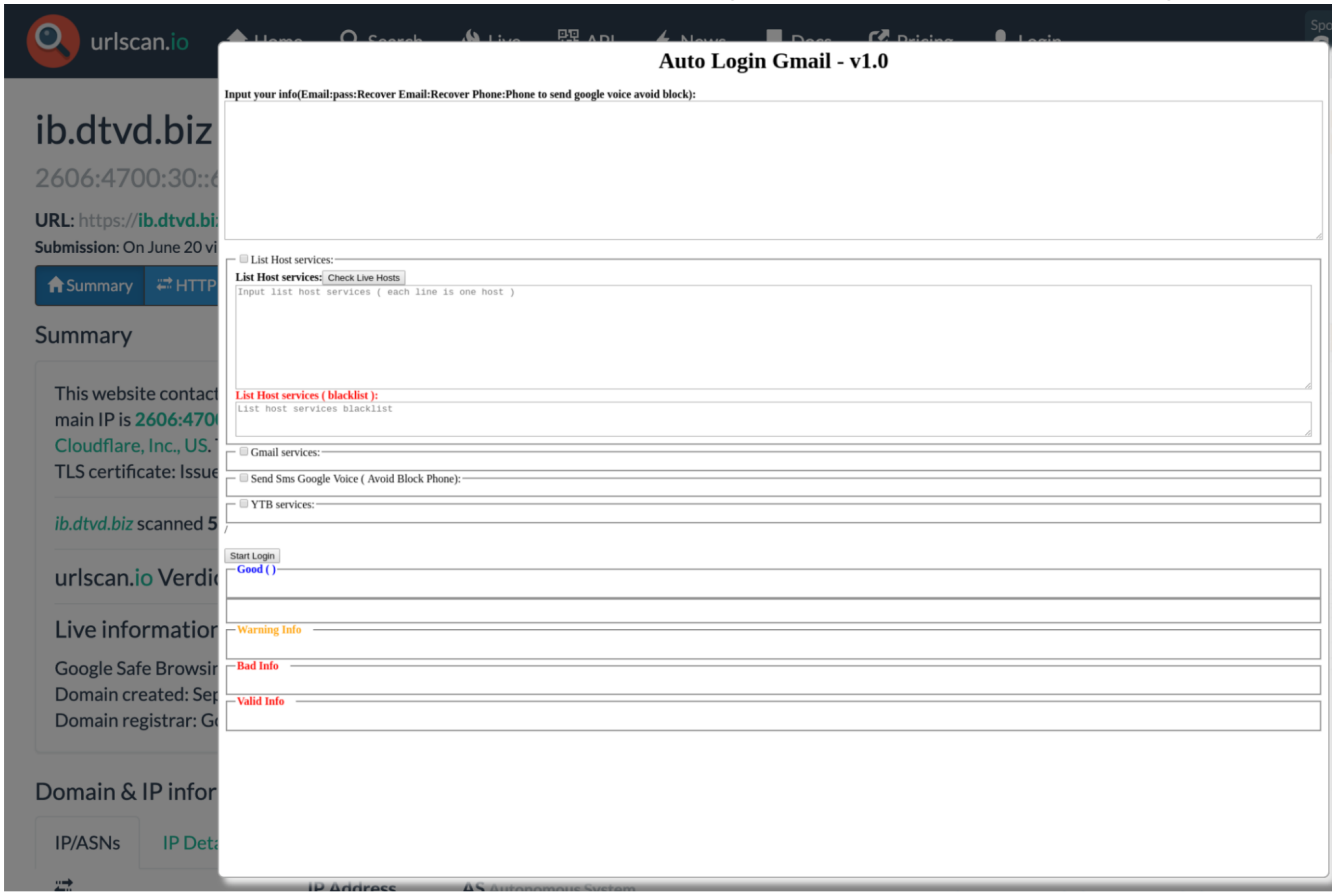


Figure 30: UI Found on Credential Collection Site

This type of GUI would be useful for somebody who was trying to quickly validate whether the credentials entered were valid and valuable. It's likely that this was a quick app spun up by an attacker for their own campaign, but it was the only piece of control infrastructure for which I was able to find visual evidence.

Tools Used

This analysis would not have been possible without the contributions of many creators inside and outside of the security community. As such, I wanted to specifically share the tools that I used as a thank you and as a reference for others.

- Urlscan for significant plaintext site analysis and historical comparison
- NetworkSage for identifying shared infrastructure, finding an active C2 domain, and allowing users to know whether or not they were affected
- Fiddler for decrypting and reviewing communications to phishing portals
- beautifier.io for making all Javascript samples more readable
- Unpacker for unpacking all obfuscated Javascript
- CyberChef for decoding Base64-encoded data
- Regexr for testing regular expressions
- TextCompare for performing a diff between code samples