

ta458 roundpress exploits

By Greg Lesnewich, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly, and the Proofpoint Threat Research Team

Published: 2026-07-15 · Archived: 2026-07-25 02:00:49 UTC

July 23, 2026 Greg Lesnewich, Nick Attfield, Konstantin Klinger, Saher Naumaan, Mark Kelly, and the Proofpoint Threat Research Team

This is part 2 of a 2-part blog series Proofpoint is publishing about Russian espionage actors using half-click exploits to target government webmail servers. Read part 1 about TA488 [here](#), and the accompanying advisory from NSA [here](#).

Threat Research would like to thank the Proofpoint Cloudmark Authority team.

Key Findings

- The Russia-aligned threat actor TA458, the group behind [Operation RoundPress](#), continues to focus on webmail targeting using half-click exploits as a way to steal highly sensitive email data.
- A “half-click exploit” requires no social engineering, nor does it require a user to click a link or open an attachment. The targeted user must only open the malicious email in their webmail viewer to be compromised.
- TA458 has been undeterred by repeated exposure from industry and government releases about its activity.
- TA458 has access to a webmail exploit supply chain; however, it is unclear whether these exploits are developed in-house, handed down from within the GRU, or procured from a third party.
- Proofpoint followed responsible disclosure practices to alert vendors when new exploits were observed against their platforms.

Overview

TA458 is an espionage threat actor with prolific access to “half-click” cross-site scripting (XSS) exploits in webmail software. TA458 is likely aligned with Russia’s General Staff Main Intelligence Directorate (GRU). In March 2026, Proofpoint discovered TA458 exploiting a zero-day vulnerability in the SOGo webmail platform, which we reported to the vendor, Alinto; it was patched as CVE-2026-8496 in version [5.12.8](#).

TA458 primarily targets Ukrainian government and Eastern European military and government entities across Albania, Greece, Moldova, and Türkiye, with occasional targeting of chemical, telecommunications, and technology firms. TA458 continues to use SpyPress - an obfuscated JavaScript-based malware seen in Operation RoundPress - which the adversary modifies based on the targeted mailserver.

Background

TA458 expanded its webmail targeting scope since ESET’s [Operation RoundPress](#) blog in May 2025. Proofpoint observed additional TA458 targeting of Kerio Webmail and SOGo Webmail, in addition to exploits deployed against Zimbra, mDaemon, and Roundcube. StrikeReady also [observed](#) TA458 use CVE-2025-27915 as a zero-day targeting Zimbra webmail servers in a campaign from April 2025. Proofpoint tracks TA458 as distinct from [Operation](#)

[Roundish](#), which was found by Hunt.io in March 2026 and used longstanding infrastructure that [CERT-UA](#) attributed to APT28 in 2024.

Delivery and Exploitation

TA458 uses a combination of actor-controlled and compromised accounts to send exploit-laden messages. On some occasions, where visible, the threat actor uses proxy services as jump boxes to send the emails onward. Proofpoint has not observed previously targeted mailservers being used to send exploit-laden emails to new targets. It is likely that TA458 procures sending addresses in another manner, in part due to SpyPress malware only being able to set persistent access to the mailserver on mDaemon and Roundcube (see below) targets.

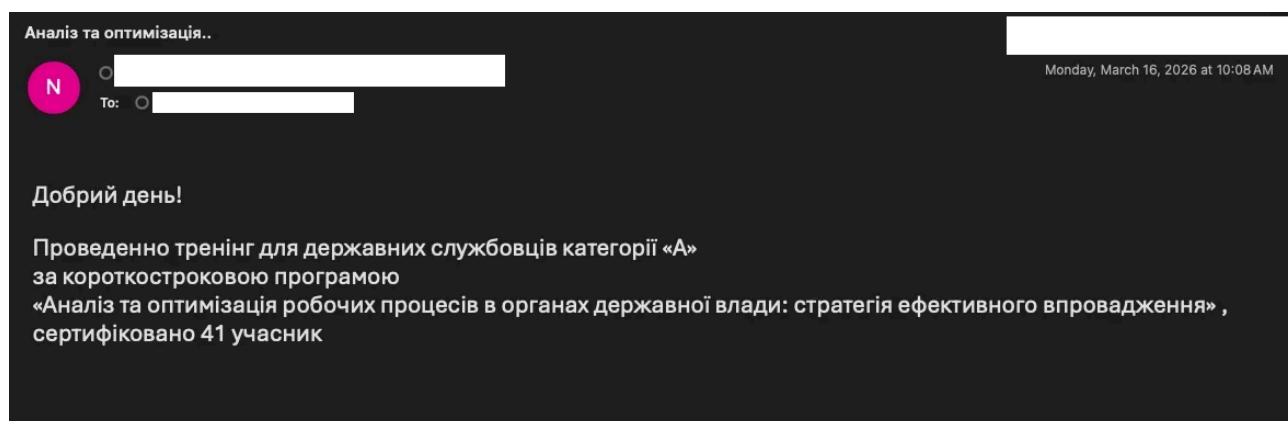


Figure 1. TA458 lure email using compromised sender to target Ukrainian entities in March 2026.

TA458 exploits this class of vulnerability by finding features in webmails that are not properly sanitized, such as event handlers that can be abused to execute arbitrary JavaScript. Proofpoint discovered TA458 exploiting vulnerabilities in Kerio and SOGo webmail platforms in March 2026 and reported our findings to the vendors. The affected Kerio webmail product was old and outdated enough that a CVE was not issued.

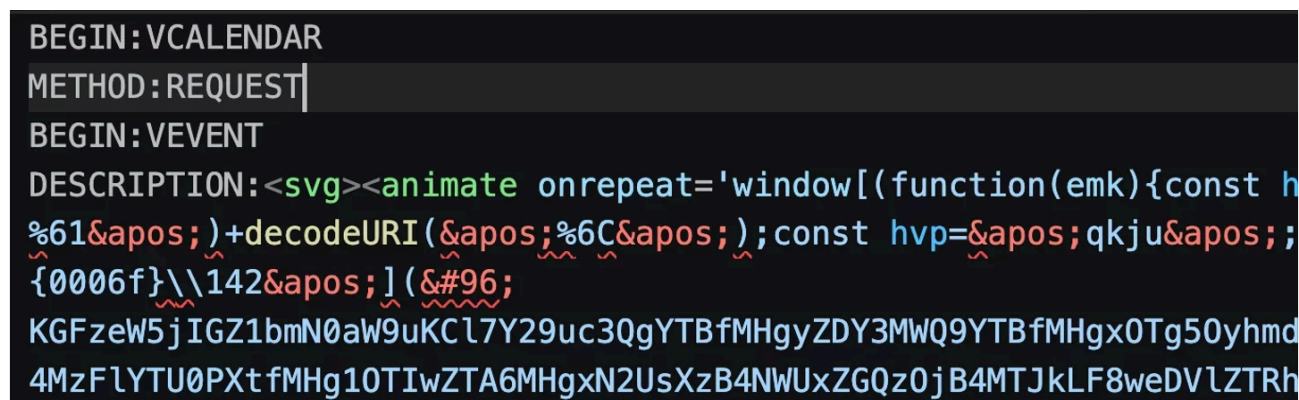


Figure 2. SOGo webmail zero-day exploit CVE-2026-8496.

In total, Proofpoint has observed TA458 exploiting the following webmail vulnerabilities:

- CVE-2025-27915: Zimbra (zero-day)
- CVE-2025-3929: mDaemon (zero-day)
- CVE-2023-43770: Roundcube (n-day)

- CVE-2024-42009: Roundcube (n-day)
- CVE-2026- 8496: SOGo (zero-day)

Since February 2026, the SpyPress malware has used a customized variant of the JavaScript obfuscation tool Obfuscator IO. The malware still varies in capabilities based on the target webmail that it is deployed against. However, the core functionality [remains consistent](#) regardless of the target: theft of credentials, contacts, and emails.

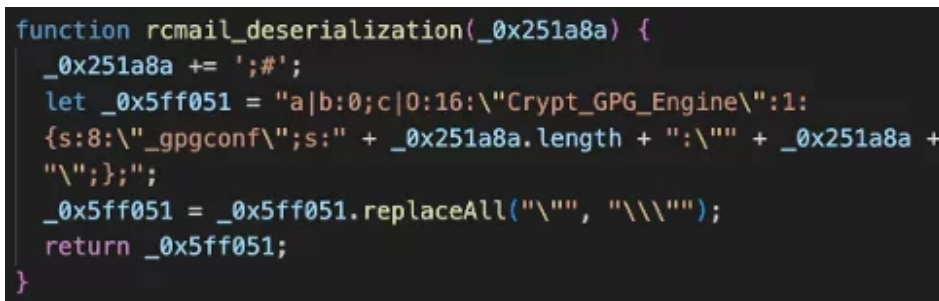


```
function a0_0x1989(_0x5c80df, _0x18ecaa) {
  _0x5c80df = _0x5c80df - 0xff;
  const _0x18737f = a0_0x1873();
  let _0x1989f5 = _0x18737f[_0x5c80df];
  if (a0_0x1989['aPHmWL'] === undefined) {
    var _0x5e449e = function(_0x1855d9) {
      const _0x543556 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/-=';
      let _0x793fbe = '',
          _0x253b16 = '';
      for (let _0x1e2b60 = 0x0, _0x212e87, _0x28a30a, _0x352b55 = 0x0; _0x28a30a = _0x1855d9['charAt'](_0x352b55++);
          _0x28a30a = _0x543556['indexOf'](_0x28a30a);
      )
      for (let _0x3a0f22 = 0x0, _0x524f5d = _0x793fbe['length']; _0x3a0f22 < _0x524f5d; _0x3a0f22++) {
        _0x253b16 += '%' + ('00' + _0x793fbe['charCodeAt'](_0x3a0f22)['toString']() * 0x10)['slice'](-0x2);
      }
      return decodeURIComponent(_0x253b16);
    };
    a0_0x1989['ccQfnS'] = _0x5e449e, a0_0x1989['vtdMRr'] = {}, a0_0x1989['aPHmWL'] = !![];
  }
}
```

Figure 3. Customized Obfuscator IO usage in SpyPress malware.

Shift to Long Term Access on Roundcube

Since at least July 2025, TA458 began removing stealing components, and swapping in interactive backdoor mechanisms to its Roundcube variant of SpyPress, to enable long-term access to the instance. SpyPress uses a second Roundcube exploit ([CVE-2025-49113](#)) that abuses Roundcube's file upload handler to trigger unsafe PHP deserialization. The deserialization allows SpyPress to use Crypt_GPG_Engine as a gadget to attacker-controlled input to the system GPG binary as a config file argument, allowing for arbitrary code execution.



```
function rcmail_deserialization(_0x251a8a) {
  _0x251a8a += ';#';
  let _0x5ff051 = "a|b:0;c|0:16:\"Crypt_GPG_Engine\":1:
  {s:8:\"_gpgconf\";s:\" + _0x251a8a.length + \":\":\"\" + _0x251a8a +
  \"\";};\";
  _0x5ff051 = _0x5ff051.replaceAll(\"\\\"\", \"\\\\\\\"\\");
  return _0x5ff051;
}
```

Figure 4. Roundcube deserialization function in SpyPress payload.

SpyPress attempts to install six distinct backdoor or persistence mechanisms with that exploit, which is likely built as a series of fallbacks to ensure the server is able to facilitate at least one of the backdoor methods. These persistence mechanisms are as follows:

1. Open a reverse shell with PHP fsockopen() to TA458 C&C
2. Open a reverse bash shell with bash -i >& /dev/tcp/ to the same C&C

3. Use PHP `get_file_contents` to fetch content from a domain hosted on the same C&C
4. Use Python `requests.get` to fetch content from the domain
5. Use `curl -k` to fetch content from the domain
6. Drop a basic PHP webshell to the following paths:

- `program/js/list.js.php`
- `program/resources/blank.gif.php`
- `plugins/password/password.js.php`
- `program/actions/mail/get.php.php`

Each command that connects to TA458 C&C servers uses a unique URI path, so the operators can understand the context of execution.

Attribution

Proofpoint assesses that TA458 is likely a Russian military intelligence operation directed by the Russian GRU. At the time of writing, there is no indication of targeting overlap in Proofpoint telemetry between TA458 and TA422 (Sofacy, APT28, Fancy Bear, Forest Blizzard), which has been [attributed to GRU Unit 26165](#).

In April 2025, France's cybersecurity agency, ANSSI, [published a document](#) providing broad context for TA422 activity targeting France. In conjunction with this publication, France's Ministry for Europe and Foreign Affairs published a [press release](#) that highlighted an additional GRU unit, 20728. It is plausible that TA458 is linked to Unit 20728 based on the distinct TTPs and targeting of the two clusters in our data, and the French government naming an otherwise unknown unit in its press release. Proofpoint lacks data to substantiate this hypothesis at the time of writing; however, there is a possibility of attribution to a GRU unit other than 26165.

Targeting

Proofpoint has observed TA458 continue to target government entities in Ukraine, as well as military and government installations in Eastern Europe, with targets in Albania, Greece, Moldova, and Türkiye. There has also been outlier targeting of chemical entities, telecommunications, and technology companies. It is unclear whether TA458 acquires new exploit capabilities after identifying targets running a particular webmail platform, or whether availability informs targeting decisions.

While TA458 appears to be a capable adversary from the activity described, there have been multiple instances where there was no reconnaissance of the targeted users or where exploit emails were sent to entities not running the targeted webmail server.

Outlook

The use of large language models (LLMs) will likely accelerate TA458's vulnerability discovery rate in the very short term (along with other actors using this vector). However, as these webmail providers benefit from a correlative ability to find and close bugs in their code base, the half-click vector will likely lose its overall effectiveness as the webmail providers reduce the available attack surface in the long term. TA458 will likely continue to find more obscure webmail providers to target following this shift, but eventually switch tactics to target the mailboxes as these exploitation vectors are closed.

ET rules

[2071250 - ET MALWARE JS SpyPress C2 Beacon](#)

[2071251 - ET MALWARE JS SpyPress C2 Success Callback \(PHP\)](#)

[2071252 - ET MALWARE JS SpyPress C2 Success Callback \(Python\)](#)

[2071253 - ET MALWARE JS SpyPress C2 Success Callback \(cURL\)](#)

[2071254 - ET MALWARE JS SpyPress Dropped Webshell Inbound Request \(list.js.php\)](#)

[2071255 - ET MALWARE JS SpyPress Dropped Webshell Inbound Request \(blank.gif.php\)](#)

[2071256 - ET MALWARE JS SpyPress Dropped Webshell Inbound Request \(password.js.php\)](#)

[2071257 - ET MALWARE JS SpyPress Dropped Webshell Inbound Request \(get.php.php\)](#)

[2868022 - ETPRO EXPLOIT Alinto SOGo Webmail Cross-Site Scripting via .ics Calendar Invite \(CVE-2026-8496\)](#)

[2865231 - ETPRO WEB SERVER Zimbra Collaboration \(ZCS\) Suite Cross-site Scripting \(CVE-2025-27915\)](#)

[2865595 - ETPRO EXPLOIT MDaemon Email Server XSS via img Tag \(CVE-2025-3929\)](#)

[2051827 - ET EXPLOIT RoundCube Webmail Persistent XSS Attempt \(CVE-2023-43770\)](#)

[2066621 - ET WEB SPECIFIC APPS Roundcube Webmail Cross-Site Scripting \(CVE-2024-42009\)](#)

[2867176 - ETPRO WEB SPECIFIC APPS Roundcube Webmail Cross-Site Scripting M2 \(CVE-2024-42009\)](#)

[2063428 - ET WEB SPECIFIC APPS Roundcube Post-Auth RCE via PHP Object Deserialization \(CVE-2025-49113\)](#)

Indicators

Indicator	Type	Description	First Seen
share-ya[.]space	Domain	SpyPress C&C	May 2025
xwe[.]us	Domain	SpyPress C&C	June 2025

hgmydr[.]wiki	Domain	SpyPress C&C	March 2026
xsza[.]net	Domain	SpyPress C&C	February 2026
zxzaq[.]com	Domain	SpyPress C&C	February 2026
upgybj[.]store	Domain	SpyPress C&C	February 2026
625e4c166c7a1d5a1becf56b27d4f76a2f95935cbd8d556c30a493263d10dbf8	SHA256	Exploit- laden email (CVE- 2023-43770 - Roundcube)	May 2024
a0c80cab70d6672b01710a70f93311fc1c1db2fbbf9cd6daa543c34b87e3444a	SHA256	Exploit- laden email (CVE- 2025-27915 - Zimbra)	January 2025
fb8ec4dbed14c0a91361abd82ebe9fb083615c3dbb15348f57317af7cc41dd34	SHA256	Exploit- laden email (CVE- 2025-27915 - Zimbra)	January 2025

3a449148a0e3cac604fb93210dd7d91ccf48e06ed9aae064bc53a419a84ce9ba	SHA256	Exploit-laden email (CVE-2024-42009 - Roundcube)	January 2025
8b5a4dc237a4c89042176bc89864a4c357dcdd14fa544fe6496ccb6c31cd5b7f	SHA256	Exploit-laden email (CVE-2025-3929 - mDaemon)	April 2025
6b2c02bf82087a3ca5fb7ef8046554ff29ce85d52202bdcfae2b2653aede139a	SHA256	Exploit-laden email (CVE-2024-42900 + CVE-2025-49113 - Roundcube)	March 2026
e27d1bf82249002a66395c89dbda6ec5d8df012a84b79d36fffbf7808d28878	SHA256	Exploit-laden email (CVE-2026- 8496, SOGo)	March 2026

Source: <https://www.proofpoint.com/us/blog/threat-insight/ta458-roundpress-exploits>