

Investigation

stormshield.com/news/investigation-on-the-emeditor-supply-chain-attack

Stormshield Customer Security Lab

February 9, 2026



Investigation on the EmEditor Supply Chain attack

Published on: 09 02 2026 | Modified on: 13 02 2026

2 minutes

A recent article by Trend Micro (trendmicro.com/fr_fr/research/26/a/watering-hole-attack-targets-emeditor-users.html, published at Jan 22, 2026) about the EmEditor ([emeditor.com](https://www.emeditor.com)) supply chain attack caught our attention, as watering hole attacks are rather rare.

Stormshield's CTI Team investigated the shared indicators and found enough material to extend Trend Micro's article.

The following table is a reminder of the indicators provided in the Trend Micro's report. We started following these addresses and found following information as of 6th of February, 2026:

Domains with similar names	Resolved IP addresses
emeditorjp[.]com	5[.]101.82.118
emeditorgb[.]com	5[.]101.82.159
emeditorde[.]com	46[.]28.70.245

Looking at passive DNS resolution, we found the following additional resolutions matching these IPs:

Resolved IP addresses	Other domains with similar names
5[.]101.82.118	emeditorjapan[.]com
5[.]101.82.118	emedorg[.]com

5[.]101.82.159	emeditorltd[.]com
46[.]28.70.245	emedjp[.]com

All domains show the same pattern:

- A domain name starting with emed characters, masquerading as a domain related to EmEditor
- A .com TLD (Top Level Domain)
- Registration through NameSilo LLC on 22nd of December, 2025
- NS records pointing to ns1.dnsowl[.]com, ns2.dnsowl[.]com or ns3.dnsowl[.]com

As we can see, not all IP addresses changed.

Pivoting

Using Validin (validin.com/), we found that the response banner for emeditorde[.]com is particular because some headers are duplicated:

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 Dec 2025 22:40:29 GMT
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
vary: Accept-Encoding
content-encoding: gzip
Strict-Transport-Security: max-age=63072000
Content-Security-Policy: frame-ancestors 'self';
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000
Content-Security-Policy: frame-ancestors 'self';
X-Content-Type-Options: nosniff
```

Going further with Validin, we found that the domain emeditorde[.]com exposed HTTP headers hashed as `b97d5024adab17ceffe134f9ea877bf5` and some other domains also share this behavior:

- n8n.kraski-event[.]ru (with a known URL `https://n8n.kraski-event[.]ru:443/gate/start/e805d522`): `b97d5024adab17ceffe134f9ea877bf5`
- keyactivate[.]cc (with a known URL `https://keyactivate[.]cc:443/gate/start/e805d522`): `b97d5024adab17ceffe134f9ea877bf5`

At the time of the investigation, both domains resolved to the same IP: `64[.]188.83.146`. Unfortunately, both domains gave a 1-byte answer, so we could not go further.

We expanded our research on VirusTotal, with a search for URLs similar to the one described in the Trend Micro's report. We could not find anything else related to URL portion `"gate/init"` (used by the C2 server `cachingdrive[.]com`, as mentioned by Trend Micro). However, we found another domain with the query `entity:url path:/gate/start/` which pivots onto `hxxp://nc7d8p7u8j3n4hgm[.]com/gate/start/efeb550a`.

Domain	Resolves to IP address
nc7d8p7u8j3n4hgm[.]com	185[.]82.218.112

This domain was registered on 19th October 2025 through NameCheap and has NS records pointing to `dns1.registrar-servers[.]com` / `dns2.registrar-servers[.]com`.

The URL delivers a PowerShell script, just like the infection chain reported by TrendMicro. The script uses the same obfuscation schemes that the ones in the initial report, and the URL is `hxxps://nc7d8p7u8j3n4hgm.com/gate/init/efeb550a/{MACHINEGUID}`.

We assess with high confidence that this domain is an early stage for the EmEditor campaign, as it shares the same inner workings: a PowerShell script with the hash `ceb31976b8040cad5d5db3856466d198d3c0ea5bc904ae05c509b3b6de72e1c8`.

Conclusion

Putting all the information together, we finally get this table:

Types	Resolve to IP addresses	Domain names	Hashes	New since Trend Micro's article?	Co
Domain	emeditorjp[.]com	5[.]101.82.118	-	No	Hiç
Domain	emeditorjapan[.]com	5[.]101.82.118	-	Yes	Hiç
Domain	emedorg[.]com	5[.]101.82.118	-	Yes	Hiç
Domain	emeditorgb[.]com	5[.]101.82.159	-	No	Hiç
Domain	emeditorltd[.]com	5[.]101.82.159	-	Yes	Hiç
Domain	emeditorde[.]com	46[.]28.70.245	-	No	Hiç
Domain	emedjp[.]com	46[.]28.70.245	-	Yes	Hiç
Domain	n8n.kraski-event[.]ru	64[.]188.83.146	-	Yes	Hiç
Domain	keyactivate[.]cc	64[.]188.83.146	-	Yes	Hiç
Domain	nc7d8p7u8j3n4hgm[.]com	185[.]82.218.112	-	Yes	Hiç
File	-	-	ceb31976b8040cad5d5db3856466d198d3c0ea5bc904ae05c509b3b6de72e1c8	Yes	Hiç

All this information proves **that the attackers continued their activities even after being exposed by Trend Micro**. Every customer using either Stormshield Network Security's IP reputation or [Breach Fighter](#) is already protected from this threat.

Thanks for reading us.

Tags : [Cybersecurity - by Stormshield](#)

Last articles

[APT35 plays the same music again](#)

26 09 2025

[Technical analysis of ransomware Crypt888](#)

09 04 2024

[HiddenEyeZ cybercrime group: identity card](#)

25 05 2023

[See all articles from Technical posts](#)

Read more

[Alert](#)

[19 01 2026 Security alert CVE-2026-21858 : Stormshield Products Response](#)

[Products & Services](#)

[18 12 2025 With the TEMPEST classification, Stormshield reaffirms its commitment to digital sovereignty and strategic autonomy.](#)

[Opinion articles](#)

[08 12 2025 Cybersecurity and digital sovereignty: can Europe regain control?](#)