

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)  
> Security (<https://www.bleepingcomputer.com/news/security/>)  
> Pro-Ukraine hackers use Docker images to DDoS Russian sites

---

## Pro-Ukraine hackers use Docker images to DDoS Russian sites

---

By  
**Bill Toulas**  
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

May 4, 2022

06:14 AM

0

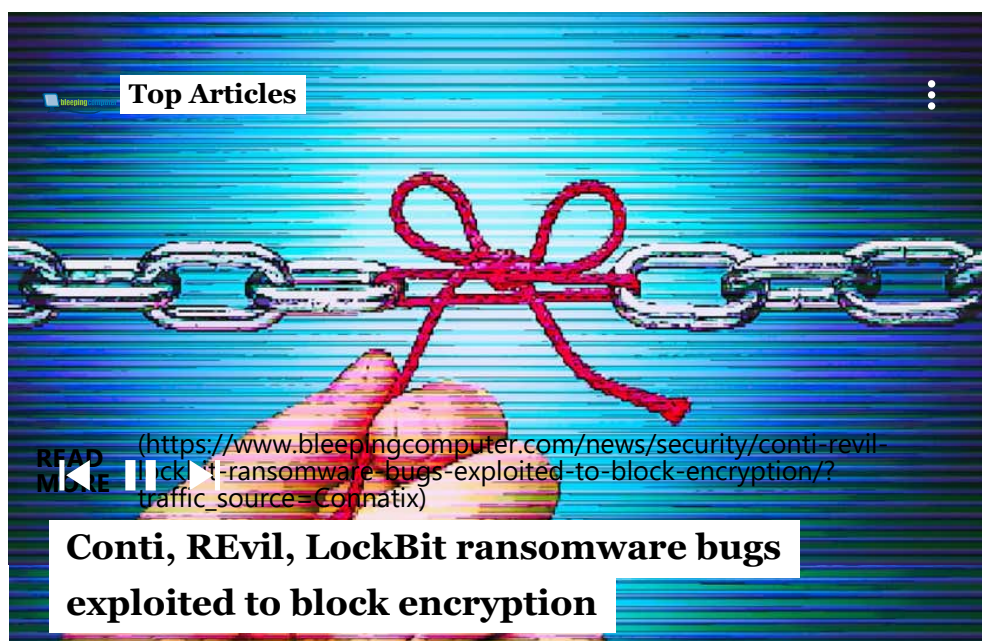


Docker images with a download count of over 150,000 have been used to run distributed denial-of-service (DDoS) attacks against a dozen Russian and Belarusian websites managed by government, military, and news organizations.



Behind the incidents are believed to be pro-Ukrainian actors such as hackers, likely backed by the country's IT Army.

DDoS cyberattacks aim to cripple operations of by sending out more requests than the target can handle and becomes unavailable to legitimate clients.



## Targeting Docker APIs

Among the 24 domains targeted include that of the Russian government, the Russian military, and Russian media like the TASS news agency.

Two Docker images involved in the attacks were spotted by threat researchers at cybersecurity company CrowdStrike, who observed them being deployed between February and March 2022.

Targeting exposed Docker APIs isn't anything novel, as cryptocurrency mining gangs like Lemon\_Duck

(<https://www.bleepingcomputer.com/news/security/docker-servers-hacked-in-ongoing-cryptomining-malware-campaign/>) and TeamTNT (<https://www.bleepingcomputer.com/news/security/teamtnt-hackers-target-your-poorly-configured-docker-servers/>) have been doing it for years.

Unfortunately, there's a plethora of misconfigured or poorly secured Docker deployments out there, allowing threat actors to hijack the available resources for their purposes.

CrowdStrike noticed that its honeypots with exposed Docker Engine APIs were infected by two malicious images fetched straight from the Docker Hub repository.

The images are named "*erikmnl/stoppropaganda*" and "*abagayev/stop-russia*", and have been downloaded 50,000 times and 100,000 respectively. The numbers don't necessarily reflect the volume



of compromised hosts, which remains unclear at this time.

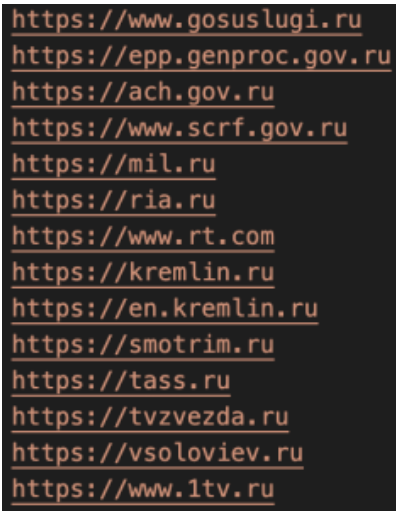
Image Name	Image Digest
abagayev/stop-russia	af39263fe21815e776842c220e010433f48647f850288b5fe749db3d7783bcb0
abagayev/stop-russia	f190731012d3766c05ef8153309602dea29c93be596dcde506e3047e9ded5eae
erikmnkl/stoppropaganda	aacbb56f72616bbb82720cb897b6a07168a3a021dd524782ee759bbec3439fda

Filename	SHA256 Hash
bombardier	6d38fda9cf27fddd4511d80c237b86f87cf9d350c795363ee016bb030bb3453
stoppropaganda	3f954dd92c4d0bc682bd8f478eb04331f67cd750e8675fc8c417f962cc0fb31f

Three samples of the two images on Docker Hub (CrowdStrike)

“The Docker image contains a Go-based HTTP benchmarking tool named bombardier with SHA256 hash 6d38fda9cf27fddd4511d80c237b86f87cf9d350c795363ee016bb030bb3453 that uses HTTP-based requests to stress-test a website. In this case, this tool was abused as a DoS tool that starts automatically when a new container based on the Docker image is created.” - CrowdStrike

The targets for the DDoS attacks were picked randomly at first but later versions of the images came with a time-based selection and a hardcoded list of targets, which were hit in one-hour assaults.



Portion of the targets list  
(CrowdStrike)

Due to the type of the operation and the targeting scope, CrowdStrike suggests that this campaign is very likely backed by the Ukraine IT Army or similar hacktivists.



Deploying these DDoS attacks may attract retaliatory action from pro-Russia hackers, which could lead to lengthy and damaging service disruption.

To help admins detect the unwanted activity, CrowdStrike has provided the following Snort rule:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "Detects DoS HTTP request sent by erikmnkl/stoppropaganda tool"; flow:to_server, established; content:"Mozilla/5.0 (Windows NT 10.0|3B| Win64|3B| x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36"; http_header; content:"GET"; http_method; classtype:trojan-activity; metadata:service http; sid:8001951; rev:20220420;)
```

**Snort rule to detect HTTP requests (CrowdStrike)**

## Related Articles:

A YouTuber is encouraging you to DDoS Russia—how risky is this?  
(<https://www.bleepingcomputer.com/news/security/a-youtuber-is-encouraging-you-to-ddos-russia-how-risky-is-this/>)

Russian defense firm Rostec shuts down website after DDoS attack  
(<https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/>)

Google: Russia, China, Belarus state hackers target Ukraine, Europe  
(<https://www.bleepingcomputer.com/news/security/google-russia-china-belarus-state-hackers-target-ukraine-europe/>)

Google: Chinese state hackers keep targeting Russian govt agencies  
(<https://www.bleepingcomputer.com/news/security/google-chinese-state-hackers-keep-targeting-russian-govt-agencies/>)

Russian hackers launch DDoS attacks on Romanian govt sites  
(<https://www.bleepingcomputer.com/news/security/russian-hackers-launch-ddos-attacks-on-romanian-govt-sites/>)

