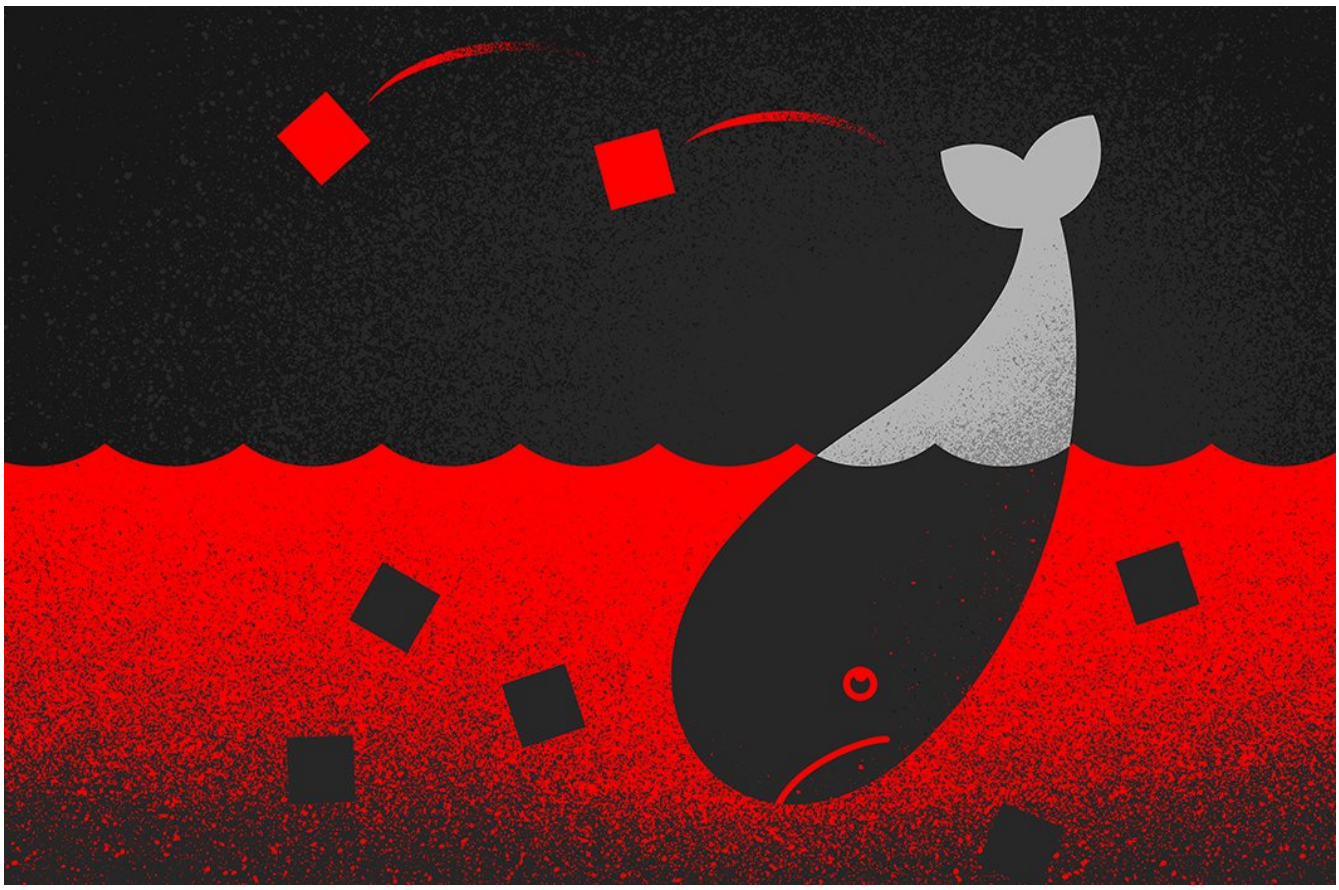
Compromised Docker Honeypots Used for Pro-Ukrainian DoS Attack

crowdstrike.com/blog/compromised-docker-honeypots-used-for-pro-ukrainian-dos-attack/

Sebastian Walla May 4, 2022



- Container and cloud-based resources are being abused to deploy disruptive tools. The use of compromised infrastructure has far-reaching consequences for organizations who may unwittingly be participating in hostile activity against Russian government, military and civilian targets.
- Docker Engine honeypots were compromised to execute two different Docker images targeting Russian, Belarusian and Lithuanian websites in a denial-of-service (DoS) attack.
- Both Docker images' target lists overlap with domains reportedly shared by the Ukraine government-backed Ukraine IT Army (UIA).
- The two images have been downloaded over 150,000 times, but CrowdStrike Intelligence cannot assess how many of these downloads originate from compromised infrastructure.
- CrowdStrike customers are protected from this threat with the CrowdStrike Falcon Cloud Workload Protection module.

Between February 27 and March 1, 2022, Docker Engine honeypots were observed to have been compromised in order to execute two different Docker images targeting Russian and Belarusian websites in a denial-of-service (DoS) attack. Both Docker images' target lists overlap with domains reportedly shared by the Ukraine government-backed Ukraine IT Army (UIA). The UIA previously called its members to perform distributed denial-of-service (DDoS) attacks against Russian targets. There may be risk of retaliatory activity by threat actors supporting the Russian Federation, against organizations being leveraged to unwittingly conduct disruptive attacks against government, military and civilian websites.

Initial Compromise via Exposed Docker Engine

The honeypot was compromised via an exposed Docker Engine API, a technique that is commonly used by opportunistic campaigns such as LemonDuck or WatchDog to infect misconfigured container engines.

Technical Analysis

The first Docker image that was observed — called `abagayev/stop-russia` — is hosted on Docker Hub. This image has been downloaded over 100,000 times, but CrowdStrike Intelligence cannot assess how many of these downloads originate from compromised infrastructure. The Docker image contains a Go-based HTTP benchmarking tool named `bombardier` with SHA256 hash

`6d38fda9cf27fddd45111d80c237b86f87cf9d350c795363ee016bb030bb3453`

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. Upon starting, the target-selection routine picks a random entry from a hard-coded target list. Later versions of this Docker image alternatively pick one of the first 24 entries of the target list, based on the current hour.

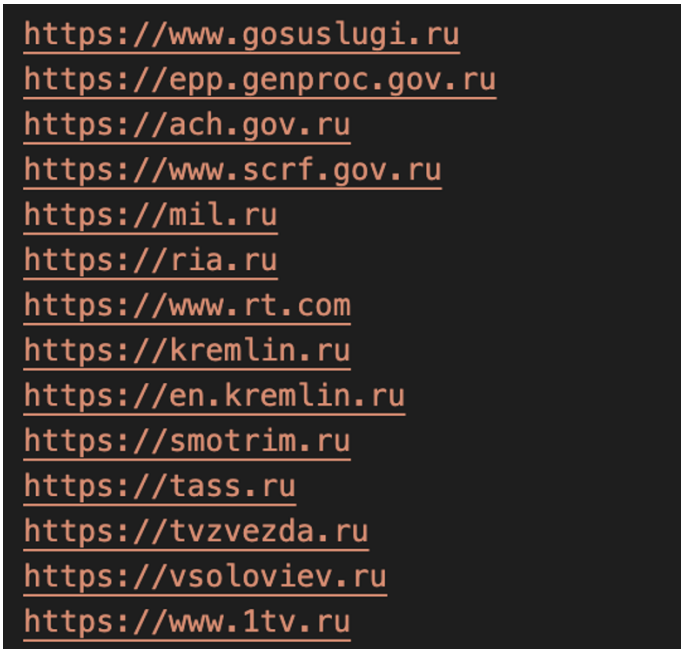


Figure 1. Excerpt of targeted websites

The deployed image was updated once on March 1, 2022. The most significant difference between the two versions of this image is that the target list was expanded. The target list contains Russian websites from the following sectors: government, military, media, finance, energy, retail, mining, manufacturing, chemicals, production, technology, advertisements, agriculture, transportation and political parties. Also on March 1, 2022, Belarusian websites from the media, retail, government and military sectors were added to the target list. CrowdStrike Intelligence assesses the activity deploying this Docker image as very likely automated based on closely overlapping timelines in the interaction with the Docker API. This assessment is made with moderate confidence, based on three separate incidents showing analogous timelines.

The second Docker image is named `erikmnkl/stoppropaganda`. This image has been downloaded over 50,000 times from Docker Hub. Again, the portion of these downloads that originated from compromised machines is unknown. The image contains a custom Go-based DoS program named `stoppropaganda` that has the following SHA256 hash

`3f954dd92c4d0bc682bd8f478eb04331f67cd750e8675fc8c417f962cc0fb31f`

that sends HTTP GET requests to a list of target websites that overloads them with requests. The attack focused on Russian and Belarusian websites in the same sectors: government, military, energy, mining, retail, media and finance. Furthermore, three Lithuanian media websites fell victim to the attack.

```
.rodata:00000000006A5FA1 aHttpsBukimevie db 'https://bukimevieningi.lt/'
.rodata:00000000006A5FBB aHttpsWwwBelnov db 'https://www.belnovosti.by/'
.rodata:00000000006A5FD5 aHttpsWwwGazpro db 'https://www.gazprombank.ru'
.rodata:00000000006A5FEF aHttpsWwwKommer db 'https://www.kommersant.ru/'
.rodata:00000000006A6009 aHttpsWwwTvrmog db 'https://www.tvrmogilev.by/'
```

Figure 2. Excerpt of targeted websites

CrowdStrike Detection

The CrowdStrike Falcon® platform protects its customers with its runtime protection and cloud machine learning models from any post-exploitation activities. As can be seen in Figure 3, the malicious DoS process from the `erikmnkl/stoppropaganda` image gets terminated by Falcon's cloud-based machine learning model, when running the Docker container on a host with the Falcon Sensor for Linux installed.

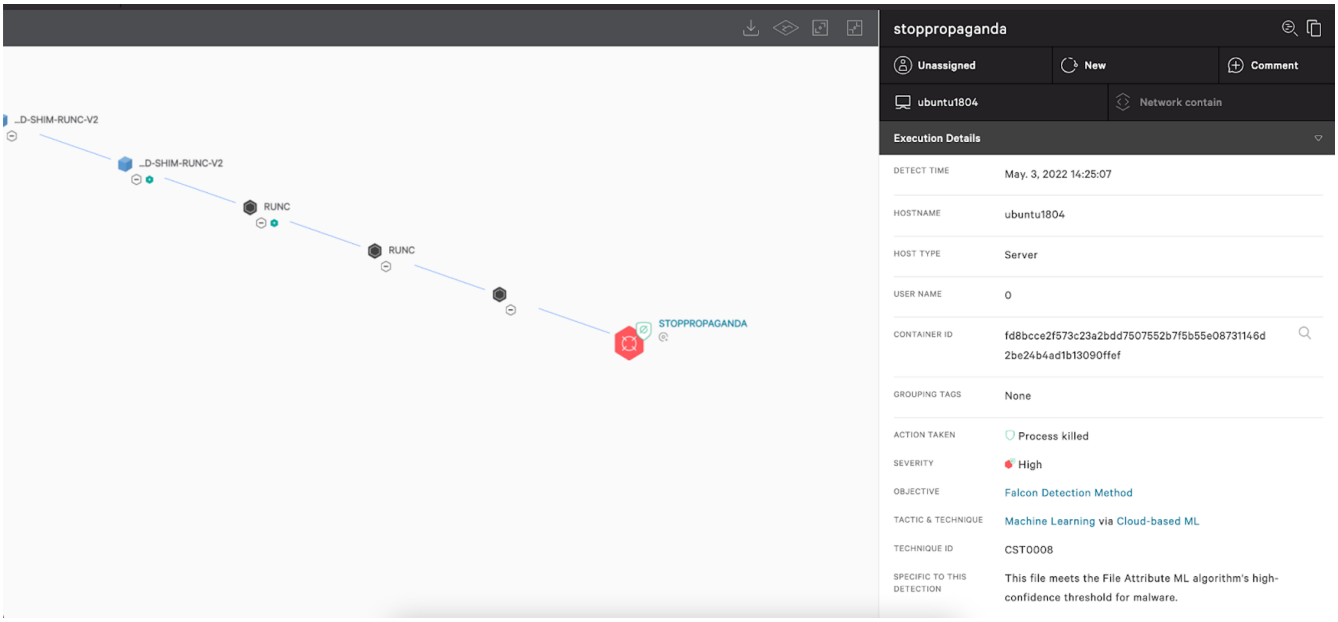


Figure 3. CrowdStrike's cloud-based machine learning model kills the malicious process (Click to enlarge)

Assessment

Both Docker images' target lists overlap with domains reportedly shared by the Ukraine government-backed UIA that called its members to perform DDoS attacks against Russian targets. CrowdStrike Intelligence assesses these actors almost certainly compromised the honeypots to support pro-Ukrainian DDoS attacks. This assessment is made with high confidence based on the targeted websites.

CrowdStrike Intelligence Confidence Descriptions

High Confidence – Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence – Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence – Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Indicators of Compromise (IOCs)

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

Filename	SHA256 Hash
`bombardier`	`6d38fda9cf27fddd45111d80c237b86f87cf9d350c795363ee016bb030bb3453`
`stoppropaganda`	`3f954dd92c4d0bc682bd8f478eb04331f67cd750e8675fc8c417f962cc0fb31f`

Snort

The following Snort rule can be used to detect HTTP requests sent by `erikmnkl/stoppropaganda`:

```
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;)
```

Additional Resources

- *Learn how you can stop cloud breaches with CrowdStrike unified cloud security posture management and breach prevention for multi-cloud and hybrid environments — all in one lightweight platform.*
- *Learn more about how Falcon Cloud Workload Protection enables organizations to build, run and secure cloud-native applications with speed and confidence.*
- *See if a managed solution is right for you. Find out about Falcon Cloud Workload Protection Complete: Managed Detection and Response for Cloud Workloads.*