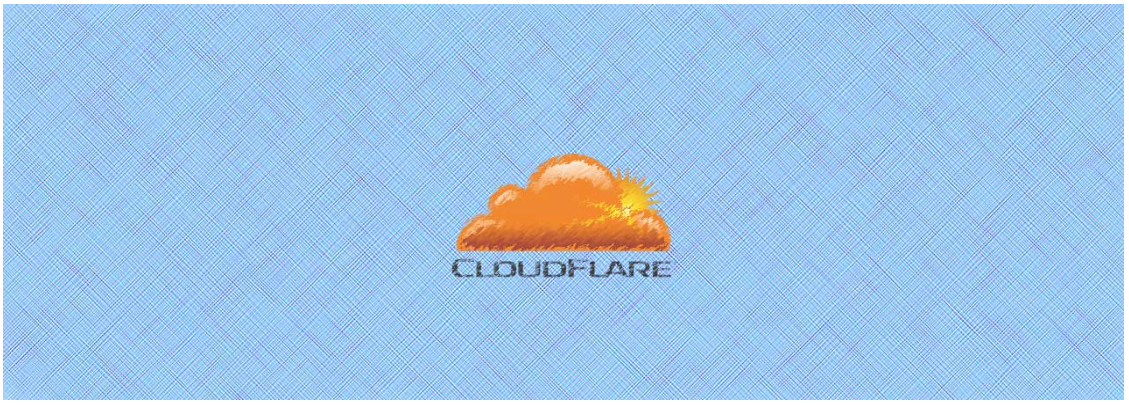
BlackWater Malware Abuses Cloudflare Workers for C2 Communication

By Lawrence Abrams

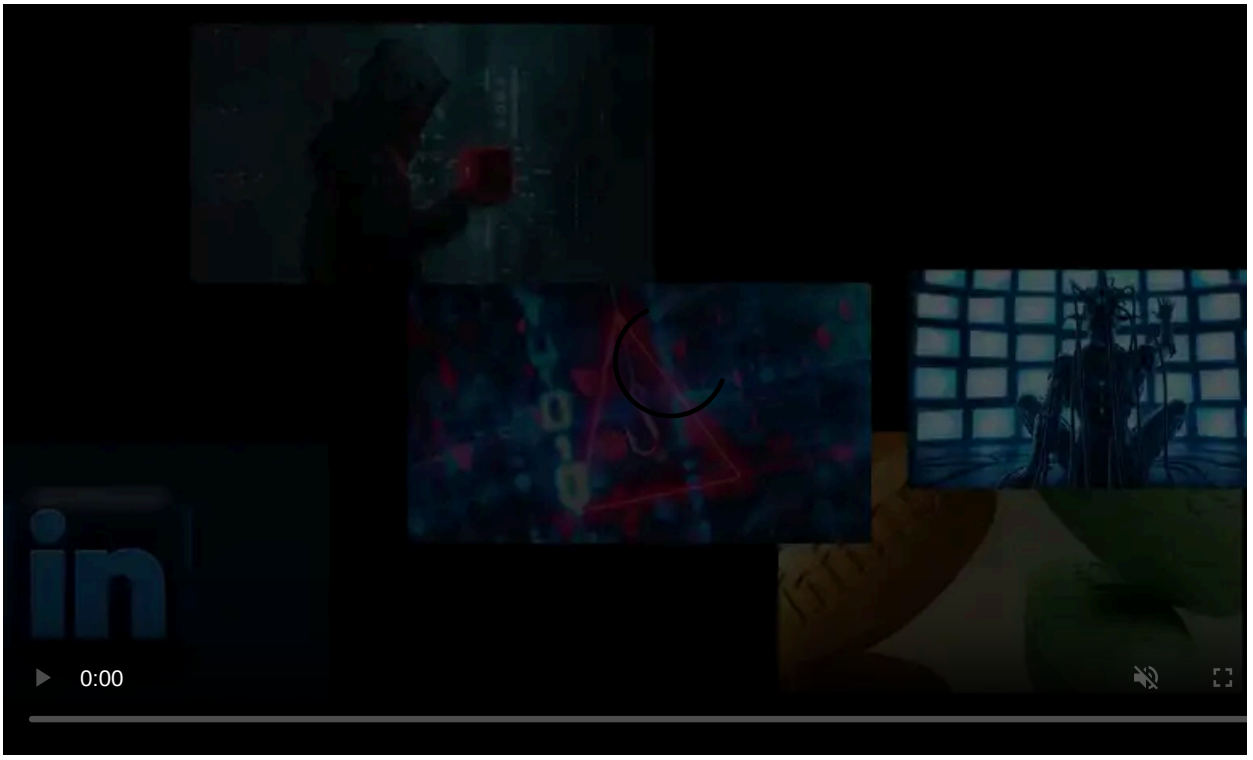
Published: 2020-03-14 · Archived: 2026-04-05 17:40:38 UTC

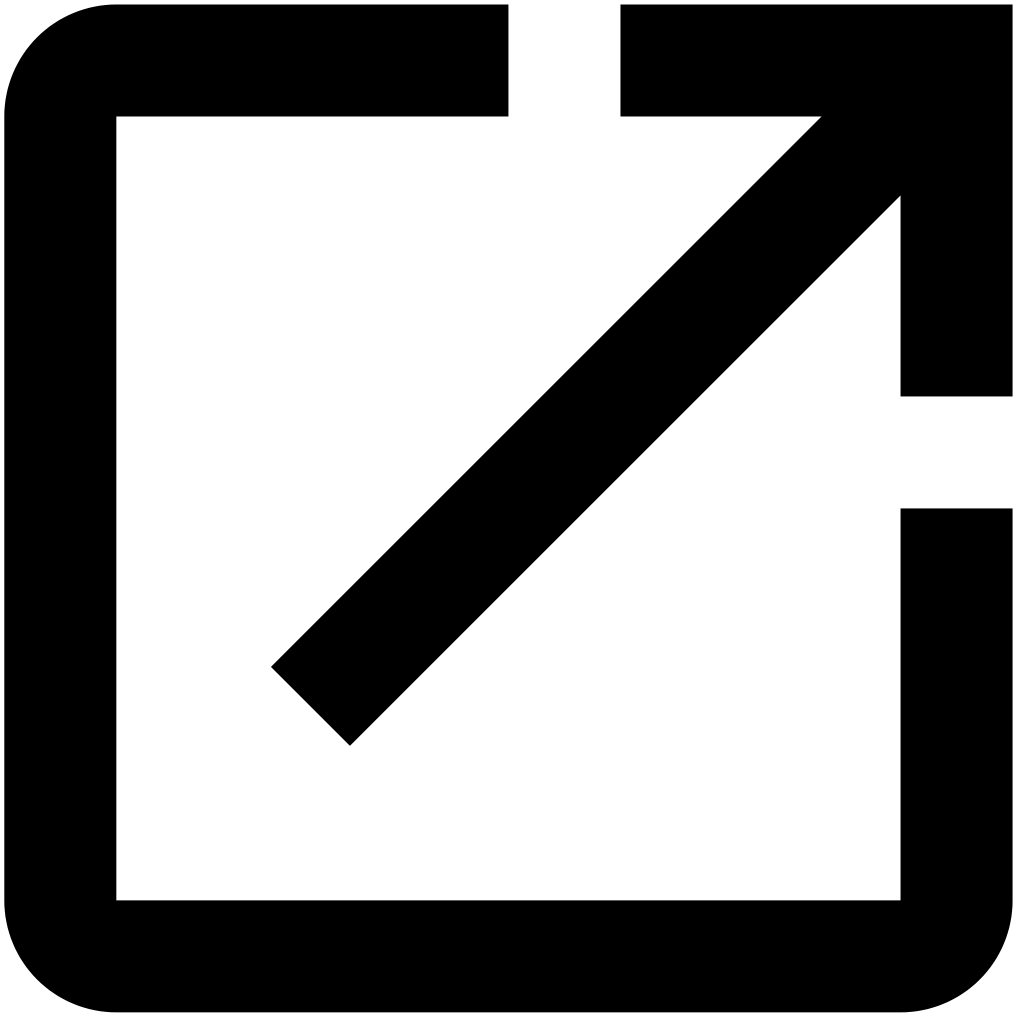


A new backdoor malware called BlackWater pretending to be COVID-19 information while abusing Cloudflare Workers as an interface to the malware's command and control (C2) server.

Cloudflare Workers are JavaScript programs that run directly on Cloudflare's edge so that they can interact with connections from remote web clients. These Workers can be used to modify the output of a web site behind Cloudflare, disable Cloudflare features, or even act as independent JavaScript programs running on the edge that displays output.

For example, a Cloudflare Worker can be created to search for text in a web server's output and replace words in it or to simply output data back to a web client.


0:00

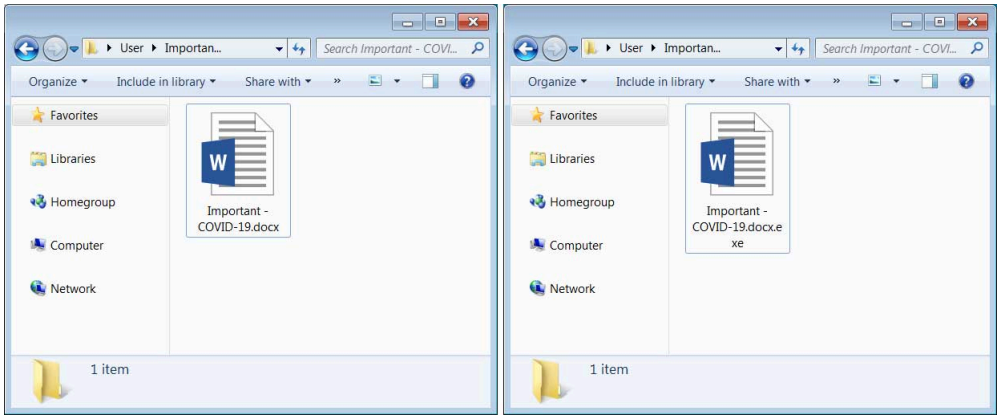


BlackWater uses Cloudflare Workers as a C2 interface

Recently MalwareHunterTeam discovered a RAR file being distributed pretending to be information about the Coronavirus (COVID-19) called "Important - COVID-19.rar".

It is not known at this time how the file is being distributed, but it is most likely being done through phishing emails.

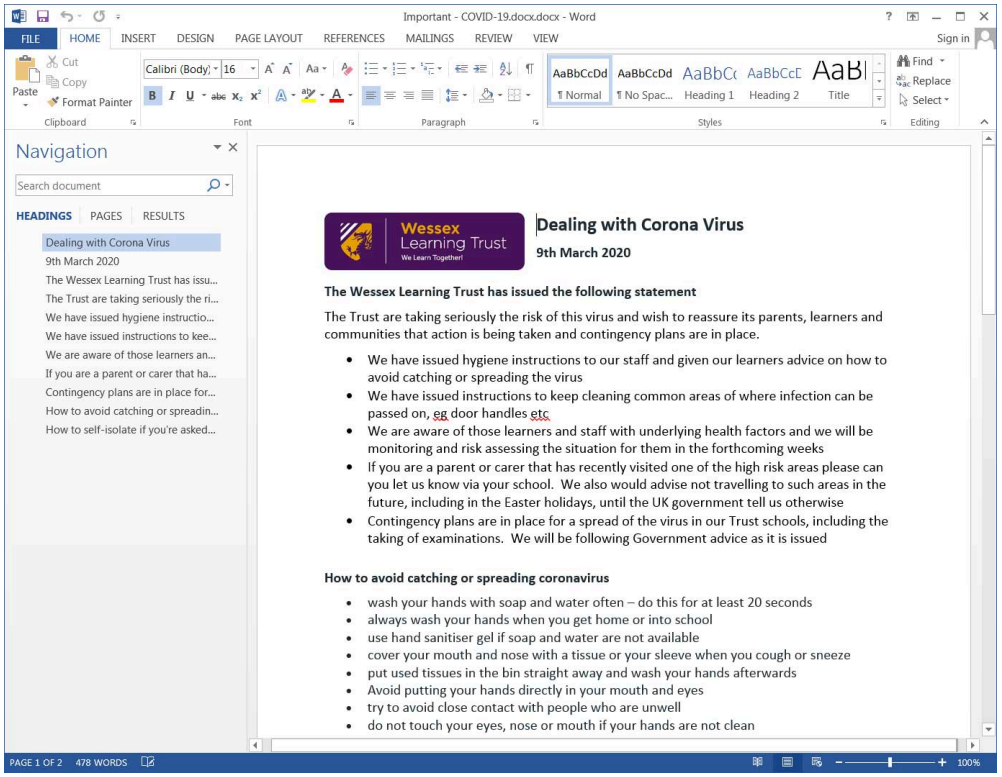
Inside this RAR file is a file called "Important - COVID-19.docx.exe" that uses a Word icon. Unfortunately, as Microsoft hides file extensions by default, many will simply see this file as a Word document rather than an executable and be more likely to open it.



Extracted file with extensions off and on

When opened, the malware will extract a Word document to the %UserProfile%\downloads folder called "Important - COVID-19.docx.docx" and opens it in Word.

The opened document is a document containing information on the COVID-19 virus and is being used by the malware as a decoy as it installs the rest of the malware and executes it on the computer.



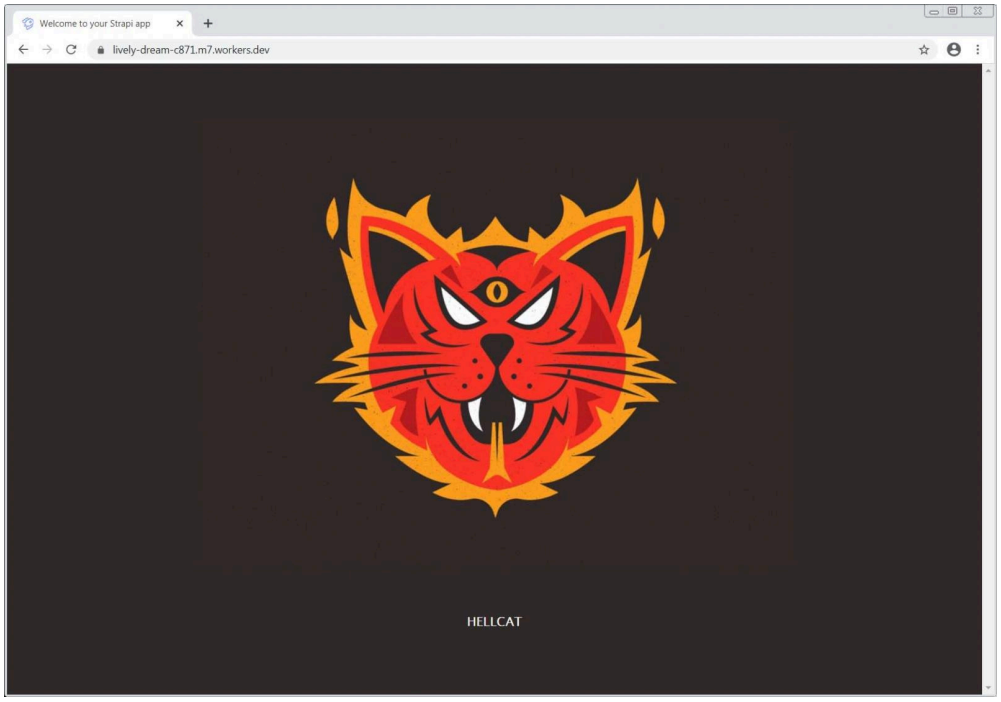
Decoy COVID-19 Information Document

While victims are reading the COVID-19 document, the malware is also extracting the %UserProfile%\AppData\Local\Library SQL\bin\version 5.0\sqltuner.exe file.

This is where things get a bit interesting as the malware is then launched using a command line that causes the BlackWater malware to connect to a Cloudflare Worker that acts as a command and control server or at least a passthrough to one.

```
sqltuner.exe lively-dream-c871.m7.workers.dev
```

If visiting this site directly, users will be shown the following 'HellCat' image.



Cloudflare worker

Head of SentinelLabs Vitali Kremez told BleepingComputer that this worker is a front end to a ReactJS Strapi App that acts as a command and control server.

Kremez stated that this C2 will respond with a JSON encoded string that may contain commands to execute when the malware connects to it with the right authentication parameters.

The BlackWater malware is, by and large, a newer generation malware taking advantage of the ReactJS Strapi App for the backend checking, leveraging Cloudflare workers resolvers and employing JSON-based parser inside its DLL passing the server argument directly. The check-ins bear the "blackwater" marker as well passing either email @ black.water or @ black64.water depending on the architecture.

The malware appears to be novel and its JSON-based parser with the newer generation ReactJS backend server architecture is indicative of the active development amid the CoronaVirus outbreak.

When we asked why they were using a Cloudflare Worker rather than connecting directly to the C2, Kremez felt it was to make it harder to for security software to block IP traffic without blocking all of Cloudflare's Worker infrastructure.

"I think this is why they employ as it returns back the legit Cloudflare proxy IP which acts as a reverse proxy passing the traffic to the C2. It makes blocking the IP traffic impossible given it is Cloudflare (unless the whole Cloudflare worker space is banned) infrastructure while hiding the actual C2."

While there is still plenty to learn about this new malware and how it operates, it does provide an interesting glimpse of how malware developers are utilizing legitimate cloud infrastructure in novel ways.

Using Cloud Workers, traffic to malware command & control servers become harder to block and the malware operation can be easily scaled as needed.

Source: https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/