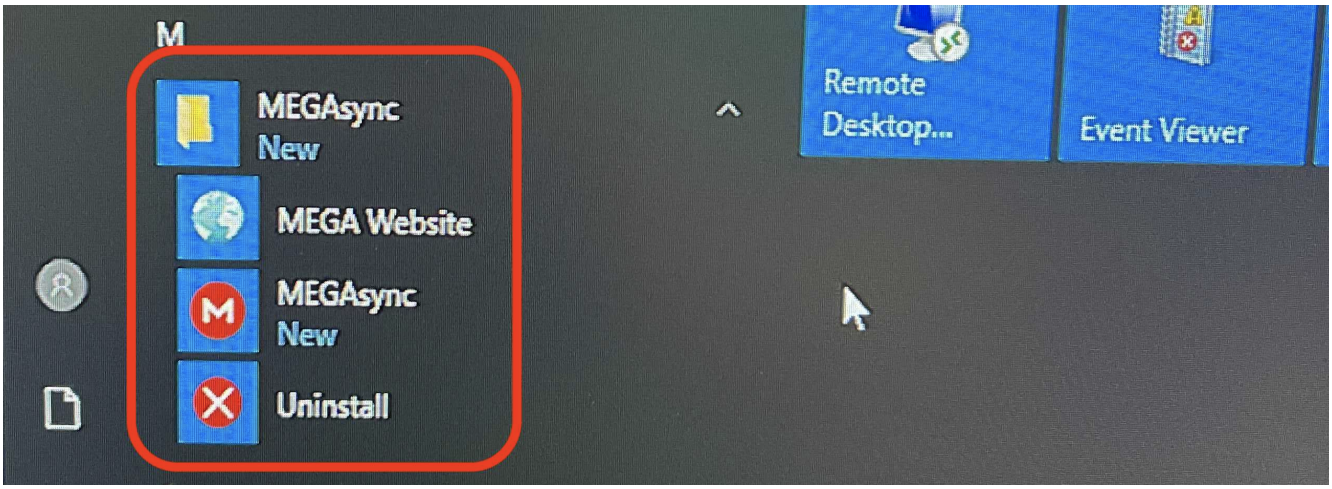
An Encounter with Ransomeware-as-a-Service: MEGAsync Analysis

blog.reconinfosec.com/megasync-analysis/

Recon's SOC recently responded to an attempted ransomware and extortion attack. It had all the markings of a nightmare scenario: malicious access through the VPN, an external server in the same IP block as the Colonial Pipeline incident, Cobalt Strike flying across the environment, and a system running an unauthorized copy of MEGAsync. We attributed the attack to a Ransomware-as-a-Service (RaaS) threat group, likely DarkSide, REvil, or their affiliates.

Through our initial response, we quickly identified and remediated compromised systems and accounts to contain the malicious activity. No files were encrypted. Our attention then turned toward an important question: what, if any, data was stolen? To answer this question, we turned to the MEGAsync logs. In this post, we'll outline our analysis of these logs so you know what to look for if you find yourself on the wrong side of an extortion attempt.



Uh oh, MEGAsync does not belong here

What is MEGA?

MEGA is a legitimate cloud backup service that has become a favorite for RaaS threat groups. Their MEGAsync software works how you would expect it: you point it at folders and shared drives and it uploads those files up to the cloud. It installs like any other Windows application. Look for it installed in places like `C:\Users\<username>\AppData\Local\MEGAsync\MEGAsync.exe` and `C:\ProgramData\MEGAsync\MEGAsync.exe`.

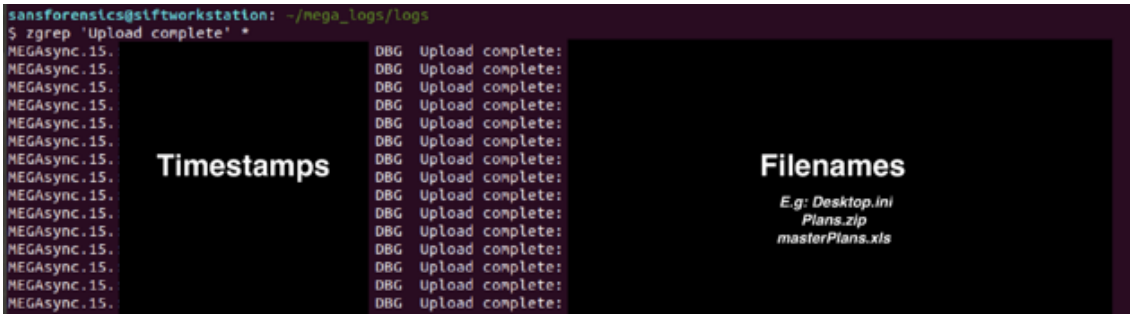
MEGA Log Analysis - Compression

MEGAsync's logs are stored in a "logs" folder in the same location as the MEGAsync.exe binary. With the exception of the most recent active log file, the older logs are compressed using gzip. You can decompress the logs using gunzip (`gunzip -S .log *`) or search them as-is using `zcat -f` and `zgrep`.

```
sansforensics@siftworkstation: ~/mega_logs/logs
$ ls -AlhrgG --time-style=+""
total 21M
-rw-r--r-- 1 1.5M  MEGAsync.log
-rw-r--r-- 1 849K  MEGAsync.9.log
-rw-r--r-- 1 853K  MEGAsync.8.log
-rw-r--r-- 1 852K  MEGAsync.7.log
-rw-r--r-- 1 852K  MEGAsync.6.log
-rw-r--r-- 1 851K  MEGAsync.5.log
-rw-r--r-- 1 853K  MEGAsync.4.log
-rw-r--r-- 1 854K  MEGAsync.3.log
-rw-r--r-- 1 851K  MEGAsync.2.log
-rw-r--r-- 1 850K  MEGAsync.1.log
-rw-r--r-- 1 5.0M  MEGAsync.16.log
-rw-r--r-- 1 1.2M  MEGAsync.15.log
-rw-r--r-- 1 855K  MEGAsync.14.log
-rw-r--r-- 1 857K  MEGAsync.13.log
-rw-r--r-- 1 852K  MEGAsync.12.log
-rw-r--r-- 1 850K  MEGAsync.11.log
-rw-r--r-- 1 852K  MEGAsync.10.log
-rw-r--r-- 1 854K  MEGAsync.0.log
sansforensics@siftworkstation: ~/mega_logs/logs
$ file MEGAsync.9.log
MEGAsync.9.log: gzip compressed data, from TOPS/20
sansforensics@siftworkstation: ~/mega_logs/logs
$ file MEGAsync.log
MEGAsync.log: ASCII text, with CRLF line terminators
```

MEGA Log Analysis - Identifying Stolen Files

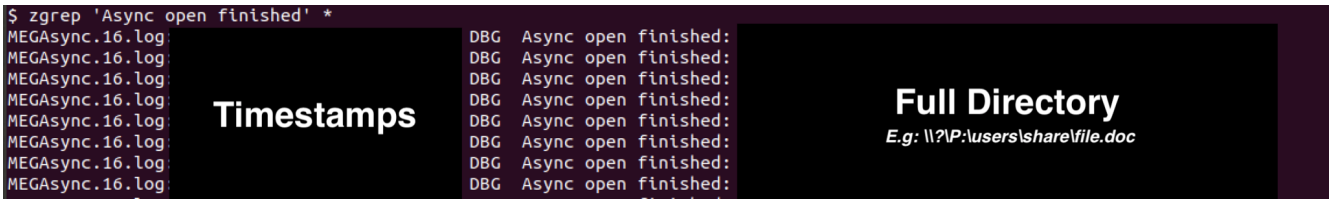
MEGA keeps track of the file successfully uploaded and logs the entries as "Upload complete:" We can search for these files using zgrep (`zgrep 'Upload complete' *`):



To count the number of uploaded files, pipe the zgrep results to wc and note the first number (`zgrep 'Upload complete' * | wc`):

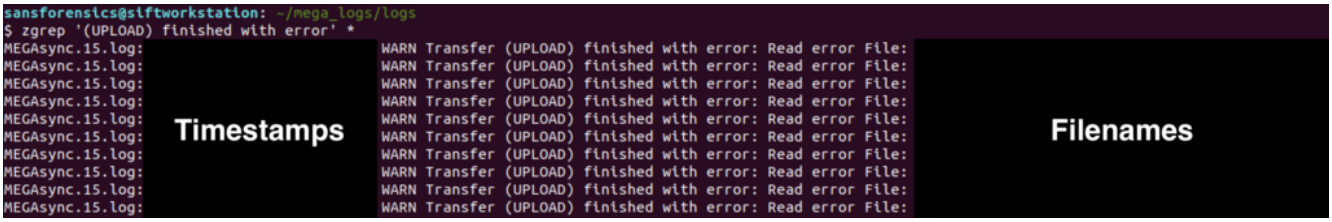
```
sansforensics@siftworkstation: ~/mega_logs/logs
$ zgrep 'Upload complete' * | wc
    263    2348   28165
```

However, this only gives us the filenames, not the full folder path and drives that those files came from. We can identify the full file locations by reading the "Async open finished" events. We believe these events are recorded as the files are queued but are not yet uploaded. These entries are important because they show the specific systems, folders, and files that the attacker targeted.



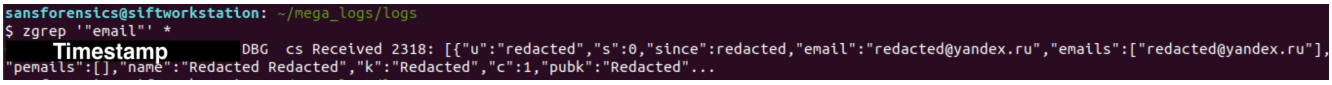
MEGA Log Analysis - Identifying Failed File Uploads

Just because a file was queued, does not mean the upload was successful. In our case, many files failed to upload after we severed the system's network connection. We can identify these failed uploads by searching the logs for "(UPLOAD) finished with error"



MEGA Log Analysis - Identifying the Attacker's Account

An interesting entry appears if you search for "email" or "emails." Though we could not confirm it, the entry appears to reveal the yandex.ru email account that the attacker used to authenticate with MEGA.



Conclusion

Examining the MEGA logs is a useful for investigating data theft and and extortion incidents. If your organization does not have a legitimate business case for MEGA software, consider blocking it. Configure EDR tools to detect or prevent its use. Set up network controls to block connections to its associated domains, such as mega.co.nz, mega.io, and mega.nz.

Tags: Security, MEGAsync

Written by Andrew Cook

Director of Security Operations