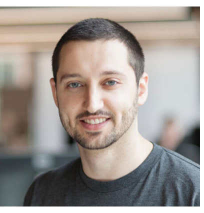
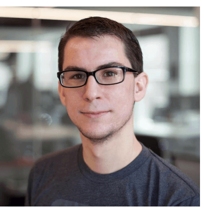
RESOURCES • BLOG

THREAT DETECTION



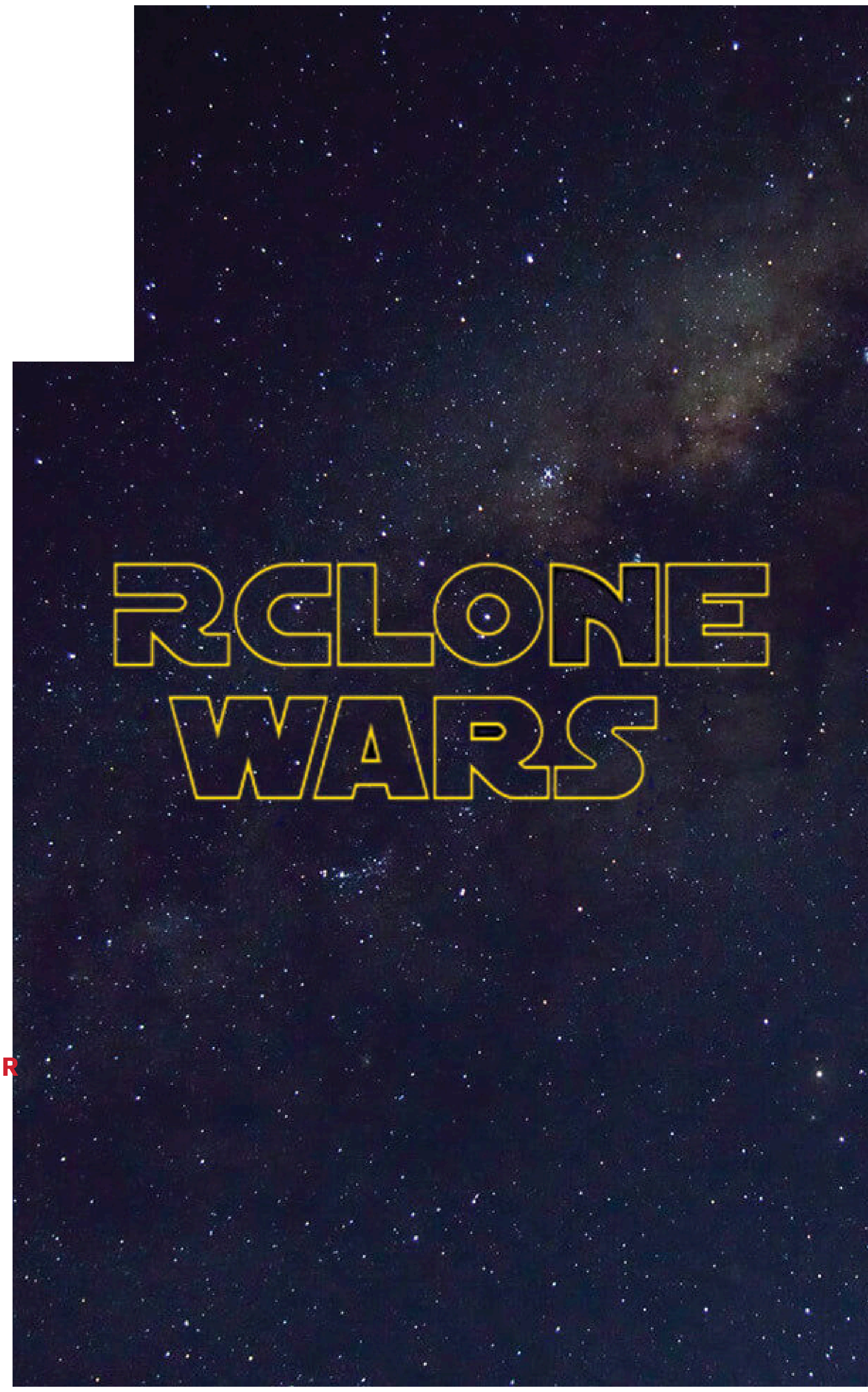


Transferring leverage in a ransomware attack

Defenders can sabotage double extortion ransomware schemes by detecting unusual file transfer utilities such as Mega and Rclone.

JUSTIN SCHOENFELD • AARON DIDIER

Originally published May 4, 2021. Last modified July 19, 2024.



Ransomware has always been about leverage, and sometimes, just encrypting files is enough to get a payment. However, as organizations have gotten better about data backup and recovery practices—by implementing policies like the "**3-2-1 rule**," for example—ransomware operators find themselves having to apply more and different kinds of leverage.

A so-called "**double extortion**" scheme, where an adversary encrypts files and threatens to leak stolen data, is one prominent example of this. In fact, the extortion side of these schemes is proving so effective that **one prominent ransomware group** recently announced that it would stop encrypting files and focus entirely on extortion moving forward.

While piling extortion on top of ransomware is an effective way of increasing leverage, it also adds conspicuous opportunities for detection in the form of illicit file transfer activity. This

With the growing number of data backup solutions, it can be hard to decipher where ransomware operators might choose to store their newly stolen data. Detection can be a particular challenge when adversaries choose to use services that are common in enterprise environments, like Google Drive or Amazon S3. Luckily for us though, they very frequently use cloud storage services that aren't normal in enterprise environments. And even when adversaries exfiltrate your data to seemingly normal cloud storage providers, they often do so with unusual file transfer utilities.

Red Canary has **observed Mega.io** used as an exfiltration destination in multiple incident response engagements this year. In these attacks, we've also witnessed adversaries leveraging legitimate file transfer utilities that Mega provides for free to its customers, making it easy for users to upload files. We've identified exfiltration to file sharing services via other tools as well, but we're going to focus entirely on Mega-related tools, like **MegaSync** and **MegaCmd**, and on the open source, cross-platform utility **Rclone**.

Asking the right questions

Even if our focus is somewhat limited, the detection principles included in this article can be readily abstracted and applied to additional file transfer utilities and other legitimate tools that are being co-opted for evil. Simply alerting on the use of any of these tools is trivial, and we include various binary metadata below that you can use to accomplish just that. Unfortunately, our experience across many short term incident response engagements is that adversaries generally try to evade simple security controls by **renaming these tools**.

As such, you'll need to understand the following:

- The authorized file sharing services and utilities in your environment
- The file sharing services and tools used in your environment, authorized or not
- The normal installation file paths for these tools
- The legitimate binary metadata associated with these tools
- The behaviors typically associated with these tools, including if and where they make network connections

Mega provides users with end-to-end encryption of files, a free basic storage tier, and a suite of tools used to transfer files remotely. Rather than hassling with hosting their own file sharing servers, adversaries would rather make use of already existing cloud storage, especially ones that allow semi-anonymous payment via cryptocurrency like Bitcoin. Simply blocking network connections to Mega-related IP addresses might be a viable security control in certain environments, but detecting the actual file transfer utilities that adversaries leverage will offer better defense-in-depth against illicit data transfer.

One such utility is Mega's main client application MegaSync, which is designed for routine file transfers and operates similarly to other cloud storage software such as Google Drive and Dropbox. In addition to MegaSync, we've also observed adversaries using the interactive command line variant known as MegaCmd. This tool offers many of the same capabilities as MegaSync but from the command line.

Establishing the baseline

Under normal circumstances, you can expect MegaSync to have the following attributes:

METADATA ATTRIBUTE	VALUE
Process name	`megasync.exe`
Process path	`C:\Users\{user}\AppData\Local\MEGAsync\MEGAsync.exe`
Description	MEGAsync
Internal name	`MEGAsync.exe`

It’s important to understand these baseline attributes because adversaries rarely execute tools like MegaCmd or MegaSync under their original filename. In this way, successful detection requires that you are able to determine the true identity of a given process regardless of what it claims to be. In other words, you might achieve a good detection outcome by identifying processes based on metadata like their internal name and then alerting when the internal name and the presented process name do not match. Similarly, you may be able to achieve success by looking for file path deviations.

Overt use of Mega

Adversaries often rename MegaSync to circumvent application controls in environments where the utility is not approved for use. However, this isn’t always the case. Trend Micro has reported that the **Nefilim ransomware** simply drops MegaSync into its normal file path under its normal name. If MegaSync isn’t approved software in your environment, then you may be able to detect its use by looking for the execution of a process that is `megasync.exe` from a path that includes the following: `\\AppData\\Local\\MEGAsync`

On top of client applications such as those provided by Mega, many ransomware families may use other software or built-in operating system utilities to exfiltrate data. We’ll use Mega as the example here, but you could just as well replace `mega.io` with whatever service you want to look out for. Since blocking a domain outright is trivial, we’ll assume that you’re okay with web browsers making network connections to Mega but want to know when anything else does.

If that’s the case, you can look for execution of any process that is **not** `chrome.exe`, `firefox.exe`, `safari.exe`, `opera.exe`, `iexplore.exe`, `microsoftedge.exe`, `microsoftedgecp.exe`, `browser_broker.exe`, `msedge.exe`, or `brave.exe` initiating a network connection to the domains `mega.io` or `mega.co.nz`.

Abnormal installation paths

In some instances, adversaries will execute MegaSync under its real name but from an unusual installation path. A detection analytic for identifying relocated copies of MegaSync execution may look something like this:

- *Binary named* `megasync.exe`
- *File execution path does not include* `AppData\\Local\\MEGAsync\\`

If there are circumstances in which it’s acceptable for Megasync to run from an abnormal directory, then consider tuning your detection logic accordingly.

Renaming MegaSync

- *Look for the execution of a process that is not named* `megasync.exe` *but that executes with any any of the following corresponding metadata:*
    - *a binary internal name that is* `megasync.exe`
    - *a binary product name that is* `MEGAsync`
    - *a binary description that is* `MEGAsync`

The following image shows the execution of `meg.exe`. However, examining binary metadata reveals that `meg.exe` was in fact a renamed instance of MegaSync.

Rclone detection

Shifting our focus away from Mega-specific tooling, it wouldn't be a blog post about exfiltration if we didn't shine a light on the cross-platform, open source file transfer utility known as Rclone. Once a ransomware operator has hooked an organization, Rclone helps them reel in their catch. Without the ability to cut the data loose, any attempts at double extortion go out the window.

So, what makes Rclone so special? Its versatility. Once an adversary drops it on an endpoint, modifying the exfiltration destination is trivial. Adversaries can also choose from a list of built-in command flags that will perform various actions, or they can opt to supply their own configuration file and avoid the need to execute with various command line flags. As an example, maybe using a cloud storage provider is not an option because of a technical control that disallows network connections to the adversary's hosting provider of choice. Rclone makes it very simple to use file transfer protocols such as FTP or SFTP, effectively enabling adversaries to move files wherever they want. See the Appendix for a list of known and supported Rclone commands at the end of this report.

Establishing the baseline

As was the case with MegaSync, understanding the binary metadata associated with Rclone is a necessary first step if you want to detect adversaries who rename the tool. Under normal circumstances, you can expect `rclone` to have the following attributes:

Process name	`rclone.exe`
Original name	`rclone.exe`
Description	Rsync for cloud storage
Internal name	`rclone`
Company name	`https://rclone.org`
Product name	Rclone

Overt use of Rclone

If Rclone isn't permitted in your environment, then you can simply look for the execution of a process named `rclone.exe`. It's worth noting that there isn't any standard path that Rclone executes from, so unfortunately we cannot pare things down further like we were able to with MegaSync.

Renaming Rclone

Red Canary has observed the execution of renamed versions of Rclone during IR engagements, in an attempt to bypass basic application controls. Taking this into account, we can begin creating detection analytics for renamed instances of Rclone, just as we did with MegaSync.

You can do so by looking for the execution of a process that is not named `rclone.exe` but that executes with any of the following binary metadata:

- a binary original name that is `rclone.exe`
- a binary description that is "Rsync for cloud storage"
- a binary internal name that is `rclone`
- a binary company name that is `https://rclone.org`
- a binary product name that is `Rclone`

The following image shows the execution of `sihosts.exe`. However, an examination of binary metadata revealed that `sihosts.exe` was in fact a renamed instance of Rclone:

Suspicious command line flags

In the interest of building resilient detection analytics, it's worth noting that metadata could be altered in some way for these binaries, enabling an adversary to circumvent some of the security controls mentioned above. Considering that, it's worth looking out for command line flags that are consistent with suspicious executions of `rclone` as well (see Appendix for the list of helpful command line perimeters).

Any time you observe these command line flags in play, it might be time to get your magnifying lens out and dig into how Rclone is being used in your environment. Of course, this can differ from one organization to the next. If you have approved legitimate use cases for Rclone in your environment, then you may have to tune your analytics accordingly.

We've had success looking for command lines including one or more of the command line parameters: `rclone`, `lsd`, `remote:`, `ftp:`, `mega`, `--config`, `--auto-confirm`, or `--multi-thread-streams` and `copy`, `config`, `create`, `lsd`, `remote`, `mega`, `user`, `pass`, `--config`, `--progress`, `--no-check-certificate`, `--ignore-existing`, `--auto-confirm`, ``--multi-thread-streams` ``, `--transfers`, `ftp:`, `remote:`, or `\\`.

The following image shows what some of these command line flags might look like in the wild:

While this is a great place to start, the Rclone project is constantly being updated with new functionality, so keeping an eye on the **ChangeLog** and **Docs** may be helpful when looking for new ways to identify the utility moving forward.

> Remember: detect or do not detect. There is no try.

Appendix

As promised, the following table includes a list of Rclone commands that may be of particular interest.

FLAG	ACTION
`sync`	Sync files to a destination
`copy`	Copy files to a destination
`config`	Specify a configuration file
`create`	Create a configuration file
`lsd`	List directories
`remote`	Defines a remote destination when building a configuration file
`mega`	Mega, the cloud provider, defined while building a configuration file
`user`	Username to authenticate to a remote destination
`pass`	Password to authenticate to a remote destination

`--progress`	Lists the progress of files being transferred
`--no-check-certificate`	Skips certificate checks when brokering a network connection
`--ignore-existing`	Ignores any files that may already exist on a remote destination
`--auto-confirm`	Yes to all confirmation prompts
`--multi-thread-streams`	Define the maximum number of streams for transferring files
`--transfers`	Defines the maximum number of concurrent transfers
`ftp:`	A predefined FTP destination, observed in direct CLI execution
`remote:`	A predefined remote destination, observed in direct CLI execution
`\\`	Not a flag, but a CLI option consistent with network shares

RELATED ARTICLES

THREAT DETECTION

Artificial authentication: Understanding and observing Azure OpenAI abuse

Apple picking: Bobbing for Atomic Stealer & other macOS malware

THREAT DETECTION

Keep track of AWS user activity with SourceIdentity attribute

THREAT DETECTION

Trending cyberthreats and techniques from the first half of 2024

Subscribe to our blog

You'll receive a weekly email with our new blog posts.

First Name

Last Name

Email Address

SUBSCRIBE ›

PRODUCTS

Managed Detection and Response (MDR)
Readiness Exercises
Linux EDR
Atomic Red Team™
Mac Monitor
What's New?
Plans

SOLUTIONS

Deliver Enterprise Security Across Your IT Environment
Get a 24×7 SOC Instantly
Protect Your Corporate Endpoints and Network
Protect Your Users' Email, Identities, and SaaS Apps
Protect Your Cloud
Protect Critical Production Linux and Kubernetes
Stop Business Email Compromise
Replace Your MSSP or MDR
Run More Effective Tabletops
Train Continuously for Real-World Scenarios
Operationalize Your Microsoft Security Stack
Minimize Downtime with After-Hours Support

RESOURCES

View all Resources
Blog
Integrations
Guides & Overviews
Cybersecurity 101
Case Studies
Videos
Webinars
Events
Customer Help Center
Newsletter

PARTNERS

Overview
Incident Response
Insurance & Risk
Managed Service Providers
Solution Providers
Technology Partners
Apply to Become a Partner

COMPANY

About Us
The Red Canary Difference
News & Press
Careers – We're Hiring!
Contact Us
Trust Center and Security

Search

info@redcanary.com +1 855-977-0686 Privacy Policy Trust Center and Security

Cookies Settings