Cyber Risk

ven., oct. 7, 2022

New M365 Business Email Compromise Attacks with Rclone

Jamie Vendel

Samuel Smoker

Rclone is a data syncing tool often used by threat actors to exfiltrate data during a ransomware attack. Typically, the actors deploy Rclone after gaining remote access to the victim's network. However, recently, Kroll experts have noted the use of Rclone in M365, using credentials stolen through network compromises or phishing attacks with minimal privileges to stealthily exfiltrate large amounts of SharePoint/OneDrive data.

Kroll experts were able to replicate an event where threat actors used Rclone to download a massive number of files in a little over one hour from SharePoint/OneDrive via a Microsoft 365 (M365) account—all without remote access to a host. Kroll discovered that in order to sync data from a server or exfiltrate SharePoint/OneDrive data, the threat actor simply needs to compromise an M365 account with sufficient privileges.

More troubling, the compromised M365 account does not necessarily need to be a global administrator account, especially in the case of overly permissive configurations; Rclone may be used with any user account.

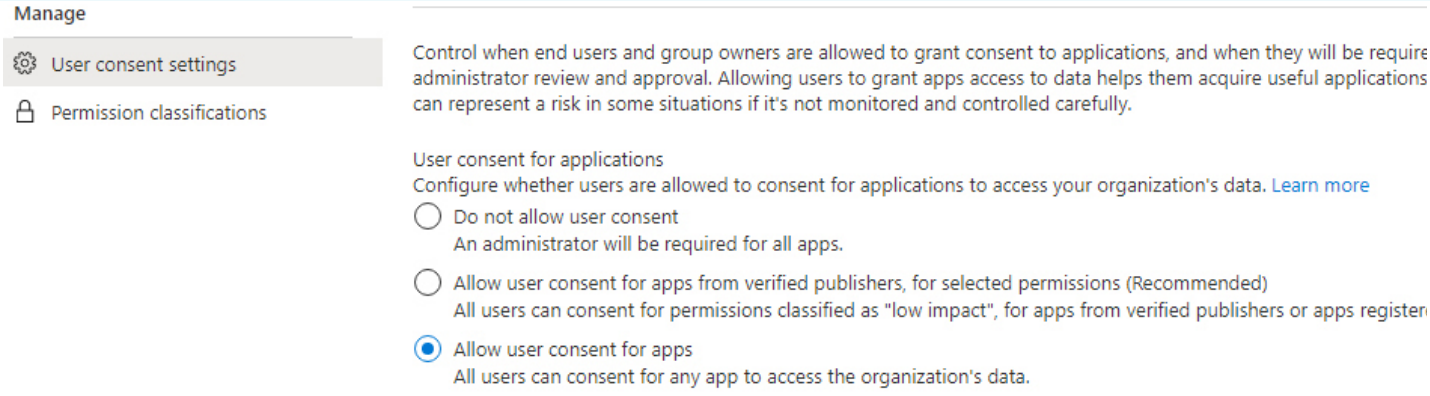

Figure 1: Settings Configured to Allow Non-Admin User Consent for Apps

Rather, the account only needs permissions to create and consent to enterprise applications. The account also needs access to the SharePoint site the threat actor is targeting with Rclone.

Digital Forensic Analysis

Kroll's testing determined that when attempting to create an enterprise application for Rclone in Azure Active Directory (AAD), the threat actor needs access to an M365 account with the ability to consent to applications.

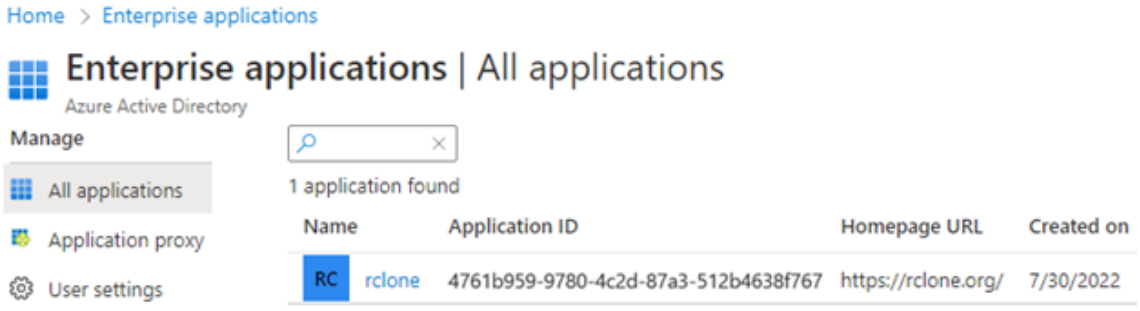

Figure 2: Rclone seen in Azure Enterprise Applications

In properly configured tenants, this means a threat actor must have a global administrator account.

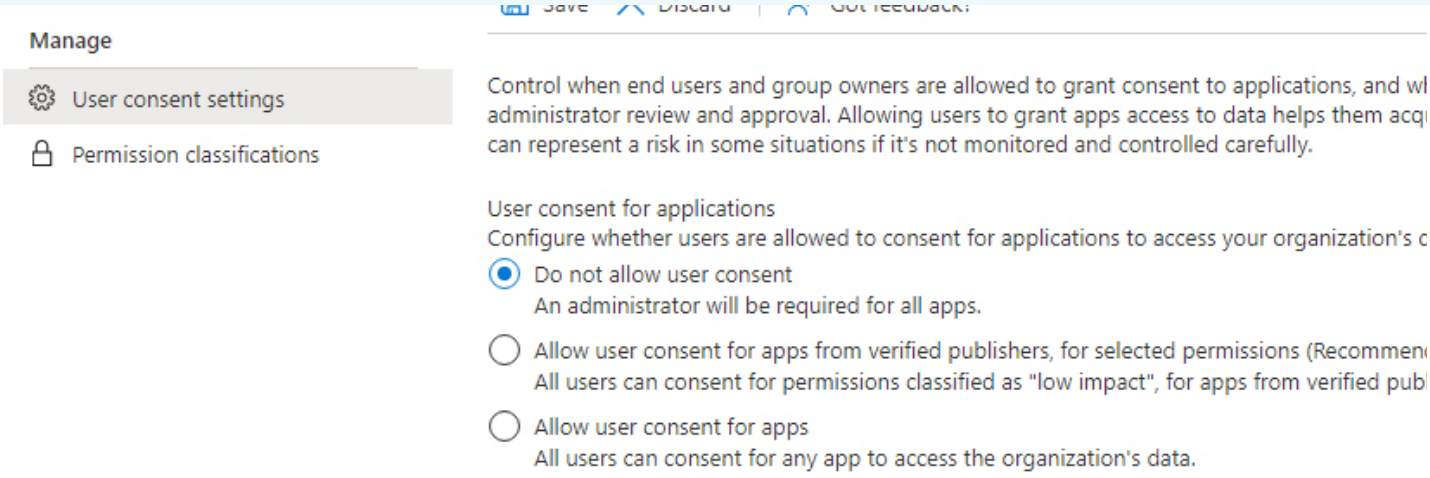

Figure 3: Properly configured settings for user consent to apps

In the non-interactive sign-in logs in AAD, our experts were able to see the Rclone application and user agent connecting to the Microsoft Graph API. Kroll observed that all users utilizing the Rclone application will appear in this log, which goes back seven days or one month, depending on AAD license level.

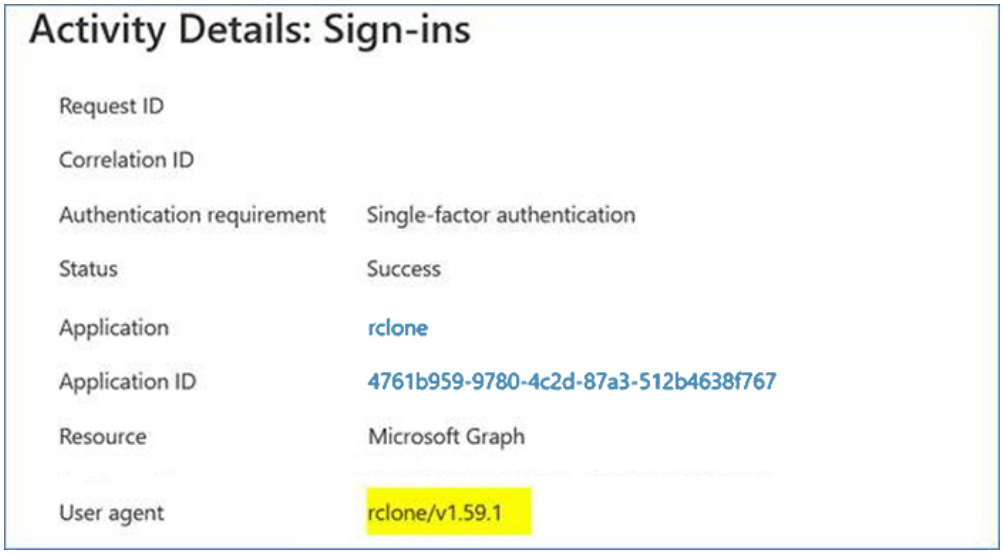

Figure 4: Application and User Agent Where Rclone Was Present

> 8/21/2022, 7:00:00	User 2	rclone	Success	Microsoft Graph

Figure 5: Azure Non-Interactive Sign-ins via the Azure Portal

Home > Enterprise applications | All applications > rclone

rclone | Sign-in logs

Enterprise Application

Date : **Last 1 month** Show dates as : **UTC**

User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins

Date (UTC)	User	Application	Status	IP address	Location
7/30/2022, 11:59:31 AM		rclone	Interrupted		Chicago, Illinois, US
7/30/2022, 12:00:26 PM		rclone	Success		Chicago, Illinois, US
7/30/2022, 12:42:05 PM		rclone	Success		Chicago, Illinois, US

Figure 6: Azure Enterprise Application Sign-Ins

Once Rclone has been installed, our experts analyzed the available M365 logs and were able to see FileDownloaded events in the unified audit log when SharePoint\OneDrive files were downloaded via Rclone within M365. For context, unified audit logs track user and account actions across all the M365 services where logging is enabled; Microsoft maintains these logs for a period of 90 days for most license levels on a first-in-first-out basis.


```
[{"CreationTime":"2022-08-22T18:54:46", Operation":"FileDownloaded","W
```


Figure 7: Unified Audit Log File Downloaded Entry

behavior customization. Since the log entries show the SharePoint path and document name, forensic examiners can find exactly what data was exfiltrated with Rclone if unified audit logging is enabled for the tenant and Rclone activity can be distinguished from other activity, such as by the user agent string.

Kroll experts tested this numerous times, and from our testing, we concluded that the logging is accurate for the files that were exfiltrated using Rclone via M365.

In Kroll's experience, actors have typically used phishing attacks to conduct financial fraud, such as misdirecting payments to the threat actors' account, rather than for collection of sensitive data for the purposes of M365 data theft/extortion. However, this new tactic gives actors a stealthy way to exfiltrate large amounts of data without alerting organizations to the attack. By sharing our findings, we hope organizations will maintain vigilance over suspicious activity in their M365 tenants, and in particular, institute more stringent permissions for application registration and consent.

Recommendations

- Review Azure Enterprise Applications regularly and remove third-party applications that are not needed for business purposes.
- Do not allow non-privileged accounts to consent for applications (An admin will be required for all application consent.)
- Only grant the Global Administrator role to dedicated administrative accounts.
- Administrators should use non-privileged accounts for email and other everyday purposes and have separate named accounts with administrator roles.
- Enable and enforce multifactor authentication (MFA) for all M365 users.
- Conduct phishing training and testing for all M365 users to raise awareness and potentially lessen the likelihood of a compromise.

Home > Enterprise applications | All applications > rclone

rclone | Audit logs
Enterprise Application

Date : **Last 1 month** | Show dates as : **UTC** | Service : **All** | Category : **All** | Activity : **All** | Add filters

Date (UTC)	Category	Activity	Status	Target(s)	Initiated by (actor)
7/30/2022, 12:00:25 PM	ApplicationManagement	Add service principal	Success	rclone	
7/30/2022, 12:00:25 PM	ApplicationManagement	Add delegated permission grant	Success	Microsoft Graph	
7/30/2022, 12:00:26 PM	UserManagement	Add app role assignment grant to user	Success	rclone	
7/30/2022, 12:00:26 PM	ApplicationManagement	Consent to application	Success	rclone	

Figure 8: Consent to Application Event

Examiners can find evidence of Rclone being used in M365 in five primary places. Be sure to check them regularly:

- Azure Enterprise Applications
- Azure Non-Interactive Sign-Ins (Check Application ID and User Agent String)
- Azure Enterprise Application Sign-Ins (Enterprise Application > Activity > Sign-Ins)
- Unified Audit Log FileDownloaded Events (Check User Agent String)
- Unified Audit Log Consent to application Events (Check for possibly compromised accounts and unfamiliar applications)

Securing email platforms and delegating proper permissions to users based on their required access is crucial to protecting your organization. Regularly providing training and ensuring MFA is enabled can help prevent threat actors from gaining access to your network.

If you suspect suspicious activity when reviewing logs, Kroll experts are available to help 24x7 via our cyber hotlines or our contact us page.

Kroll experts have identified threat actors leveraging phishing attacks to gain access to key email and administrative-level accounts, exfiltrate hundreds of gigabytes (GBs) of data, and then initiate high-pressure extortion initiatives involving clients, colleagues, senior executives and even family members.

- **Business Email Compromise Trends and Mitigation**
  While published in 2019, this article offers still relevant insight into how business email compromise attacks are targeted at non-technical executives, shares real case studies, and provides practical tips to spot wire fraud and mitigate BEC incidents.
- **Case Study: Office 365 Business Email Compromise Investigation**
  A detailed study into how a BEC against a financial services company took place, its consequences (including massive exposure of financial information), and how Kroll was able to remediate the threat and increase the organization's cyber resilience.

Cyber and Data Resilience

Incident response, digital forensics, breach notification, security strategy, managed security services, discovery solutions, security transformation.

Kroll is the largest global IR provider with experienced responders who can handle the entire security incident lifecycle.

Computer Forensics

Kroll's computer forensics experts ensure that no digital evidence is overlooked and assist at any stage of an investigation or litigation, regardless of the number or location of data sources.

Office 365 Security, Forensics and Incident Response

Digital forensic experts investigate hundreds of Office 365 incidents per year and help strengthen your security.

Cyber Risk Retainer

Kroll delivers more than a typical incident response retainer—secure a true cyber risk retainer with elite digital forensics and incident response capabilities and maximum flexibility for proactive and notification services.

Cloud Security Services

Kroll’s multi-layered approach to cloud security consulting services merges our industry-leading team of AWS and Azure-certified architects, cloud security experts and unrivalled incident expertise.

Threat Exposure and Validation

Proactively identify your highest-risk exposures and address key gaps in your security posture. As the No. 1 Incident Response provider, Kroll leverages frontline intelligence from 3000+ IR cases a year with adversary intel from deep and dark web sources to discover unknown exposures and validate defenses.

More About Kroll

About
Solutions
Trending Topics
Client Stories
Careers
Find an Expert
Locations
Media Inquiry

KROLL

KROLL

Kroll is headquartered in New York with offices around the world.

One World Trade Center
285 Fulton Street, 31st Floor
New York NY 10007

+1 212 593 1000