You Can’t Audit Me: APT29 Continues Targeting Microsoft 365

APT29 is a Russian espionage group that Mandiant has been tracking since at least 2014 and is likely sponsored by the Foreign Intelligence Service (SVR). Mandiant continues to identify APT29 operations targeting the United States' (US) interests, and those of NATO and partner countries. Despite the publicization of multiple APT29 operations, they continue to be extremely prolific. In 2022, APT29 has focused on organizations responsible for influencing and crafting the foreign policy of NATO countries. This has included multiple instances where APT29 revisited victims they had compromised years, or sometimes only months beforehand. This persistence and aggressiveness are indicative of sustained interest in this information and strict tasking by the Russian Government.

Mandiant has observed APT29 continue to demonstrate exceptional operational security and advanced tactics targeting Microsoft 365. We are highlighting several newer TTPs used by APT29 in recent operations.

Disabling Licenses

Microsoft 365 uses a variety of licensing models to control an individual user’s access to services in the Microsoft 365 suite of products. The licenses can also dictate security and compliance settings such as

log retention and Mail Items Accessed logging within Purview Audit. The most common licenses are E1, E3, and E5; however, there are a variety of other license plans and granular add-ons that make licensing in M365 complex.

For a threat actor, one of the most troublesome logging features is Purview Audit, formerly Advanced Audit. This feature, available with E5 licenses and certain add-ons, enables the Mail Items Accessed audit. Mail Items Accessed records the user-agent string, timestamp, IP address, and user each time a mail item is accessed. The audit records any type of mail access whether it is using the Graph API, Outlook, a browser, or other methodology. This is a critical log source to determine if a threat actor is accessing a particular mailbox, as well as to determine the scope of exposure. Further, it is the only way to effectively determine access to a particular mailbox when the threat actor is using techniques like Application Impersonation or the Graph API.

Mandiant has observed APT29 disabling Purview Audit on targeted accounts in a compromised tenant. Once disabled, they begin targeting the inbox for email collection. At this point, there is no logging available to the organization to confirm which accounts the threat actor targeted for email collection and when. Given APT29's targeting and TTPs Mandiant believes that email collection is the most likely activity following disablement of Purview Audit. We have updated our white paper, Remediation and Hardening Strategies for Microsoft 365 to include more details on this technique as well as detection and remediation advice. Additionally, we have updated the Azure AD Investigator with a new module to report on users with advanced auditing disabled.

MFA Takeover of Dormant Accounts

Multi-factor authentication (MFA) is a crucial tool that organizations can deploy to thwart account takeover attacks by threat actors. By requiring users to provide both something they *know* and something they *have*, organizations can significantly reduce the risk of account compromise. MFA itself, however, is not a silver bullet. Mandiant has previously discussed how threat actors abuse push-based MFA to spam users with notifications until they eventually accept the prompt and allow the threat actor access. Microsoft has recently announced that they will roll out MFA push notification with number matching to combat this.

Mandiant has begun to observe another trend where threat actors, including APT29, take advantage of the self-enrollment process for MFA in Azure Active Directory and other platforms. When an organization first enforces MFA, most platforms allow users to enroll their first MFA device at the next login. This is often the workflow chosen by organizations to roll out MFA. In Azure AD and other platform's default configuration, there are no additional enforcements on the MFA enrollment process. In other words, anyone with knowledge of the username and password can access the account from any location and any device to enroll MFA, so long as they are the first person to do it.

In one instance, APT29 conducted a password guessing attack against a list of mailboxes they had obtained through unknown means. The threat actor successfully guessed the password to an account that had been setup, but never used. Because the account was dormant, Azure AD prompted APT29 to enroll in MFA. Once enrolled, APT29 was able to use the account to access the organization's' VPN infrastructure that was using Azure AD for authentication and MFA. Mandiant recommends that organizations ensure all active accounts have at least one MFA device enrolled and work with their platform vendor to add additional verifications to the MFA enrollment process. Microsoft Azure AD

recently rolled out a feature to allow organizations to enforce controls around specific actions such as MFA device enrollment. Using conditional access, Organizations can restrict the registration of MFA devices to only trusted locations, such as the internal network, or trusted devices. Organizations can also choose to require MFA to enroll MFA. To avoid the chicken-and-egg situation this creates, help desk employees can issue Temporary Access Passes to employees when they first join or if they lose their MFA device. The pass can be used for a limited time to login, bypass MFA, and register a new MFA device.

Focus on Operational Security

APT29 continues to demonstrate exceptional operational security and evasion tactics. In addition to the use of residential proxies to obfuscate their last mile access to victim environments, Mandiant has observed APT29 turn to Azure Virtual Machines. The virtual machines used by APT29 exist in Azure subscriptions outside of the victim organization. Mandiant does not know if these subscriptions have been compromised or purchased by APT29. Sourcing their last-mile access from trusted Microsoft IP addresses reduces the likelihood of detection. Because Microsoft 365 itself runs on Azure, the Azure AD Sign-In and Unified Audit Logs already contain many Microsoft IP addresses and it can be hard to quickly determine if an IP address belongs to a malicious VM or a backend M365 service. From Mandiant's own observation it also appears that Microsoft owned IP addresses greatly reduce the risk of detection by Microsoft's risky sign-ins and risky users reports.

Mandiant has also observed APT29 mix benign administrative actions with their malicious ones. For example, in a recent investigation APT29 gained access to a global administrator account in Azure AD. They used the account to backdoor a service principal with `ApplicationImpersonation` rights and start collecting email from targeted mailboxes in the tenant. To accomplish this, APT29 added a new certificate, or Key Credential, to the service principal. Once added, APT29 was able to authenticate to Azure AD as the Service Principal and use its roles to collect email. To blend in, APT29 created the certificate with a Common Name (CN) that matched the display name of the backdoored service principal. In addition to this, they also added a new Application Address URL to the service principal. The address they added was completely benign, not needed to facilitate their malicious activities, and was related to the functionality of the application as documented by the vendor. This action demonstrates the extremely high level of preparation that APT29 takes and the extent to wish they try to masquerade their actions as legitimate.

Outlook

APT29 continues to develop its technical tradecraft and dedication to strict operational security. Mandiant expects that APT29 will stay apace with the development of techniques and tactics to access Microsoft 365 in novel and stealthy ways.