UNDERSTANDING THE DARK HALO M365 ATTACK

How the complexity of cloud-based enterprise SaaS systems allowed attackers to hide in plain sight.

SIRIUX SECRUTINY

Revision 2.2

CONTENTS

Dark Halo

Within the cybersecurity community, major attacks and campaigns are often given a name to make them memorable and more easily referenced. In December 2020, cybersecurity company Volexity coined the name Dark Halo to refer to a series of attack patterns that targeted Microsoft 365 (M365) users. These attacks leveraged the complexity of the M365 system to allow the attackers to use M365 services to identify users of interest, exfiltrate data from those users' email, then file repositories and collaboration sessions using legitimate (but poorly configured) M365 services and interfaces.

For the purposes of this report, we use the term Dark Halo to categorize the different techniques used by attackers. Within the MITRE ATT&CK Matrix for Enterprise, the attackers used M365 interfaces for the following major activities:

- Reconnaissance
- Persistence
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

SolarWinds Myopia: One Route of Many

Many journalists and technology analysts have pointed at the SolarWinds supply chain attack as the initial Dark Halo attacks. This is a myopic assessment, as the attackers could have used any of thousands of enterprise system vulnerabilities to gain access to enterprise-controlled infrastructure and then pivoted to M365. While SolarWinds was an elegant and stealthy means to gain access to many high-value targets, it was just one of many they could have used to achieve the same results with the Dark Halo campaign.

Poor Identity Provider Hygiene and Facilitating MFA bypass attacks

In nearly every cybersecurity best practices publication, Multi-factor Authentication (MFA) is considered the best solution to identity proofing within any IT system. Unfortunately, most MFA implementations within enterprises today have been of the 'set it and forget it' variety. For example, the Dark Halo attackers used their enterprise system access within the targeted organizations to copy the identity provider secret keys from the MFA system, then used those to effectively clone valid user MFA sessions. Most organizations do not have their identity provider interfaces configured to get sufficient logging information to even begin to identify whether the secret keys associated with MFA services have been copied or tampered with.

Legacy Protocols: Enabling attackers to bypass security controls

Many of the M365 tenant settings that the Dark Halo attackers manipulated within the targeted organizations focused on enabling legacy protocols to exfiltrate data without triggering any sort of Data Loss Prevention (DLP) alerts. To the security operations teams, the attackers' activities looked like legitimate older devices connecting over legacy communications protocols.

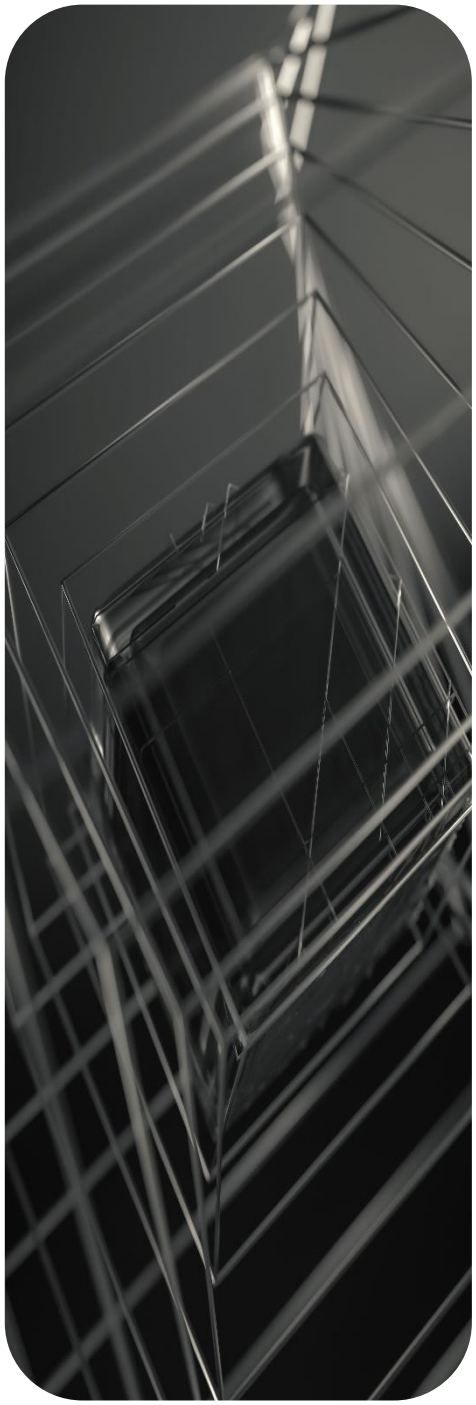
While IT leaders are always trying their best to please business users and make their ability to collaborate as smooth as possible, this approach to letting users determine which devices and protocols they get to use is a recipe for disaster. For example, in the case of Dark Halo, the attackers used decades-old email protocols such as POP3 and IMAP to set up real-time synchronization of targeted users' inboxes.

The remainder of this report covers the different M365 configuration settings that the Volexity team identified as associated with the Dark Halo attacks they responded to.

M365 Complexity and Attacker Camouflage

M365 vertigo: So Many Settings, So Little Time

In Siriux's research, we identified thousands of configurable settings for each user within the M365 platform. These range from Azure Active Directory (Azure AD) attributes to per-service configuration settings (such as those within Exchange and Intune). In addition, every SharePoint site, OneDrive share, and Teams group have additional configurable settings. The sheer magnitude of the situation can cause security teams to become disoriented as they try to assess the risks of all these configuration options.



In surveys conducted with more than 75 CISOs of Fortune 500 companies, less than 10% of these organizations have any sort of monitoring plan in place to keep track of which settings should be configured to protect information and manage privileges in the first stages of deployment, let alone on an operational basis to detect malicious configurations by attackers.

Microsoft, in its Security and Compliance Center, only focuses on the most critical security baseline settings, and the one-size-fits-all nature of their security assessment can never meet the security expectations of the diverse organizations that are relying on M365 for their collaboration needs.

The Center for Internet Security (CIS) has published an M365 Benchmark, and while it is more comprehensive in their approach than Microsoft's, it still does not contemplate security configurations and operational monitoring to detect Dark Halo attack tactics.

Siriux is offering the first widely available scanning tool that allows organizations to quickly assess the current state of their M365 tenants. The Siriux Dark Halo Scan uses Microsoft-approved API (Application Programming Interface) data gathering techniques to rapidly gather all the data relating to the attackers' Dark Halo techniques. It is a simple-to-run PowerShell script that can be downloaded and implemented in a matter of minutes.

Attacker PowerShell Activities

PowerShell – used to find data, steal it, and cover the attackers' tracks

In addition to the web-based administrative portal interfaces provided by Microsoft, there are dozens of additional ways that administrators can run commands against M365 tenants. The most popular of these is PowerShell, and Microsoft has done a hit-and-miss job at documenting them.

The attacker's PowerShell commands can be broken down into the following categories, which they used to find data, steal it, then cover their tracks:

- Data and User Discovery
- Data Exfiltration
- Attacker Activity Obfuscation

Unfortunately, most organizations do not have appropriate logging enabled to effectively perform historical threat hunting exercises to look for the forensic artefacts associated with Dark Halo attacks. The M365 default configuration only retains security and audit logs for 90 days so older data is not accessible.

If an organization begins to look for the artefacts associated with the following PowerShell commands, those tell-tale signs will only appear if the attackers were active within the last 90 days in the case of certain Discovery commands. Data Exfiltration and Activity Obfuscation settings will persist as long as M365 administrators do not reconfigure them.

Data and User Discovery PowerShell Commands

Below are the PowerShell commands that organizations should use to look for artefacts associated with attacker discovery activities:

- Get-AcceptedDomain
- Get-CASMailbox
- Get-Mailbox
- Get-ManagementRoleAssignment
- Get-OrganizationConfig

The Dark Halo attackers executed these commands to identify particular user mailboxes that were of interest to them, identify the original configuration settings, gain insight into which email domains were associated with targeted user accounts, and then verify the users' settings to ensure they could then follow up with Exfiltration and Obfuscation techniques.

Data Exfiltration PowerShell Commands

Below are the PowerShell commands and settings that organizations should review that could be associated with data exfiltration attacks:

- Set-CASMailbox
- CASMailbox: EwsEnabled
- CASMailbox: ImapEnabled
- CASMailbox: PopEnabled
- CASMailbox: ECPEnabled
- CASMailbox: MAPIEnabled
- CASMailbox: ActiveSyncEnabled
- Get-Mailbox: DelivertoMailboxAndForward
- Get-Mailbox: ForwardingAddress
- Get-Mailbox: AntispamBypassEnabled

The Dark Halo attackers used these settings and commands to create data exfiltration streams, which allowed for real-time synchronization of all targeted user email activity as well as IMAP folder-synchronization of certain SharePoint, OneDrive, and Teams content. We highly recommended that organizations immediately disable all these legacy protocols within their M365 tenant.

These revisions will prevent many legacy mobile devices from synchronizing email from the M365 tenant, but based upon the scale and scope of the Dark Halo attack, we highly recommended that all users with access to sensitive data be forced to use a modern smartphone that supports full mobile operating system updates within 4 weeks of the release of security updates by Google and Apple. Enforcing this security policy is critical when requiring the use of managed Outlook on the smartphone for mobile email synchronization and for blocking the use of iOS's and Android's native email applications.

Attacker Activity Obfuscation PowerShell Commands

Below are the PowerShell commands the Dark Halo attackers used to attempt to make it more difficult for security teams to identify their activities:

- Get-Mailbox: AuditEnabled
- Get-Mailbox: AuditLogAgeLimit
- Get-AdminAuditLogConfig: AdminAuditLogEnabled
- Get-AdminAuditLogConfig: LogLevel
- Get-AdminAudiLogConfig: UnifiedAuditLogIngestionEnabled

The attackers manipulated these settings to disable audit logging associated with targeted users' email profiles. We highly recommend that M365 administrators constantly monitor the configuration of these settings for high-value users within an M365 tenant.

Siriux Helps Simplify and Protect M365 Security

With our team's years of experience defending and running penetration tests against M365 tenants, we work every day to deliver our knowledge and expertise to our clients. By downloading and running the free Dark Halo scan, you can immediately find out the state of your M365 security settings.

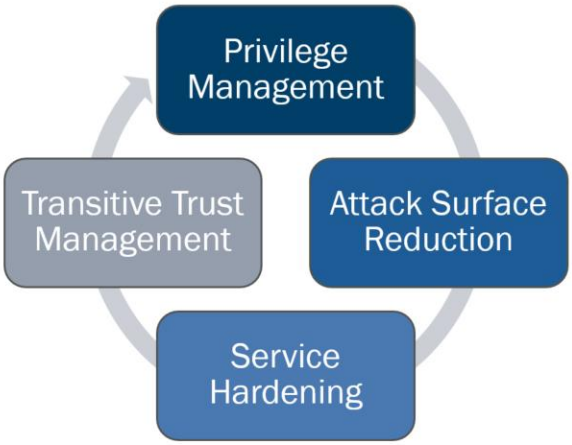
Contact siriux@secrutiny.com or use discount code 'Secrutiny' when speaking to Siriux to be introduced to our security analysts who will help you defend against the thousands of additional attack vectors that we have discovered in our research.

Siriux's Comprehensive M365 Security Assessment

Only Siriux offers a complete review of M365 security settings. Compared with competitors, which mainly focus on helping optimize billing and availability settings, Siriux's only focus areas are the confidentiality of M365 data and the integrity of M365 user identities.

Scope of Assessment

- Baseline M365 Assessment Includes:
  - Azure AD
  - Exchange Online
  - Teams/Skype for Business
  - M365 Cross-Tenant Settings
- Additional Analysis:
  - SharePoint
  - OneDrive
  - Intune



SaaS Security Posture: Not Just an M365 Problem

On a broader scale, attackers can use the same techniques associated with the Dark Halo campaign against other cloud-based SaaS platforms such as Salesforce, Workday, and ServiceNow.

Siriux is developing similar security posture management assessments for these SaaS platforms. If you are interested in being an early adopter of those offerings, please email your Secrutiny Client Director.

Get a free Dark Halo M365 Security Scan

Secrutiny and Siriux are offering free Dark Halo M365 Security Scans to find out if your M365 tenant is vulnerable to attacks like Dark Halo.

Contact siriux@secrutiny.com or use discount code 'Secrutiny' when speaking to Siriux

Website: SIRIUX.TECH