CoreView

The Anatomy of a Microsoft 365 Attack

Microsoft 365 is a Tier #01 Cyber Security Concern

Post-pandemic, Microsoft 365 is no longer just another service, it is now the backbone of the modern workplace. Workloads like Teams, SharePoint, and Exchange have never been more mission-critical. And, from a security standpoint, they have never been so exposed.

With a wide variety of workloads, configurations, and a proclivity towards open collaboration, the Microsoft 365 ecosystem has become a focus point for cybercriminals.

Nation-state attackers like Fancy Bear, APT28, and Strontium have directed a significant amount of effort to target Microsoft 365 services and the infrastructure that connects to it.

While it's true cybercriminals typically start attacks with email, the sheer variety of services that Microsoft 365 offers gives hackers an abundance of different ways to gain access and move through a tenant.

OAUTH consent phishing, public Teams and SharePoint sites, misconfigurations, and overprivileged applications all present windows of opportunity for cybercriminals that take the pressure off traditional attack vectors, and the data supports this.

Mimecast has recently reported that 94% of organizations are experiencing cyberattacks in their collaboration spaces like Teams and SharePoint.

In 2024, even Microsoft struggled to secure their tenant with the now infamous midnight blizzard attack.

In January Microsoft announced that cyber-criminals had breached their tenant and had been able to exploit excessive privileges to move through their environment.

The most troubling part of the breach is that it implies Microsoft did not detect the initial risks in their environment or the configuration changes the attackers made to elevate their privileges and establish persistence.

Cyber security and governance teams already know that Microsoft 365 presents an enormous challenge. Hidden beneath a unified brand is a complex variety of workloads with 18+ admin interfaces, 5000+ different types of configurations, an endless array of 3rd party and custom apps connecting to Entra ID, and no easy way to manage it all.

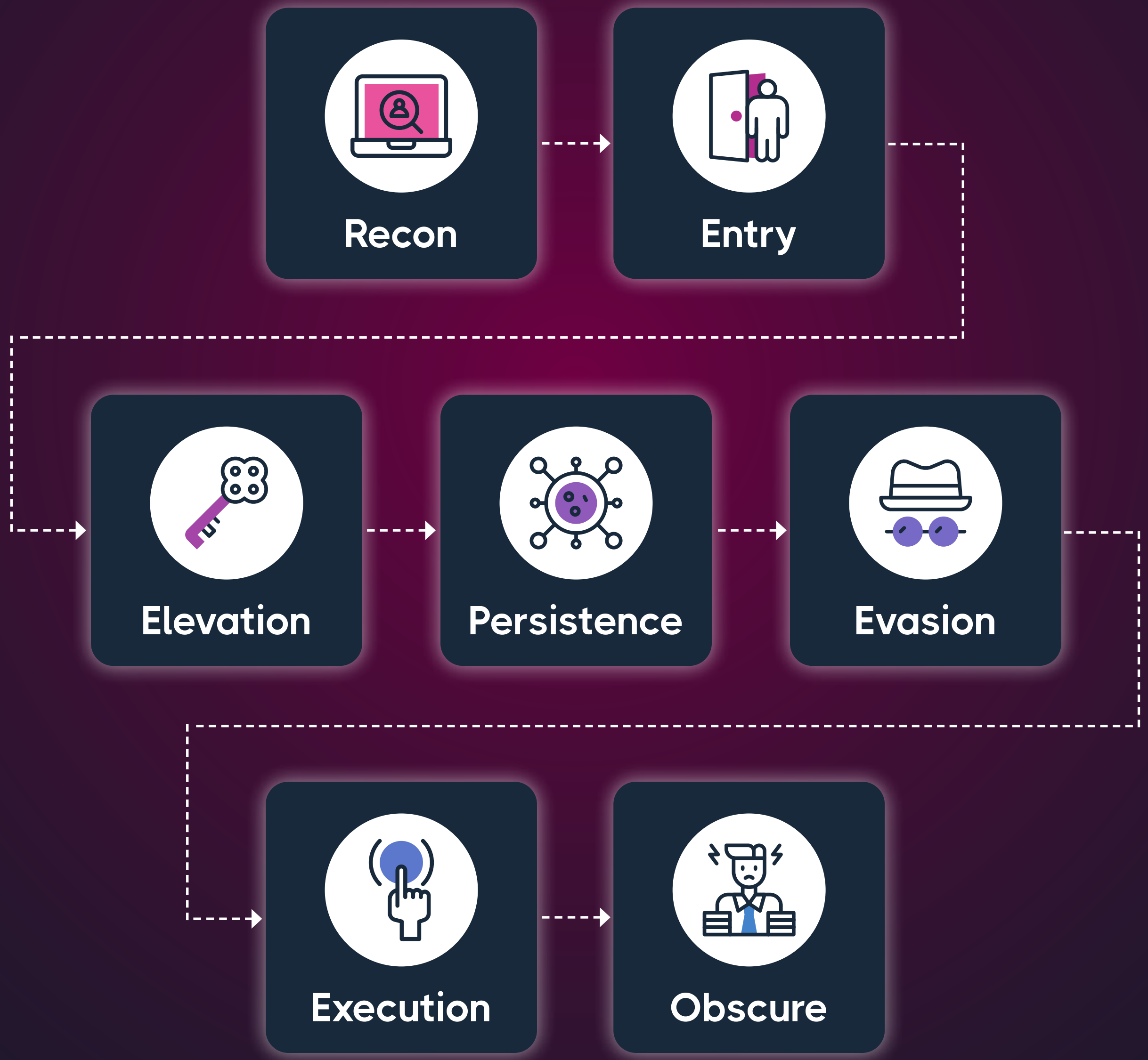
To see Microsoft struggling to maintain oversight of their environment is the ultimate reminder that this is not a talent problem.

When CoreView was founded, our objective was straightforward: we wanted to help Microsoft customers who couldn't get proper visibility of what was going on in their tenants.

A decade later, with the rising attacks on Microsoft 365, the need for enhanced visibility, risk detection, and remediation is crucial. In 2024, advanced email security must pair with dedicated oversight and security automation to ensure resilience and continuous compliance across Microsoft 365 workloads.

To this end, this whitepaper has been written to map out the various vulnerabilities a cybercriminal will look to exploit as they gain entry, elevate their privileges, and establish persistence in Microsoft 365.

The Anatomy of a Microsoft 365 Attack



Recon

Entry

Elevation

Persistence

Evasion

Execution

Obscure

Table of Contents

Part 1: **Research**

1(A): RECONNAISSANCE ON PUBLIC WEB

PROBLEM:

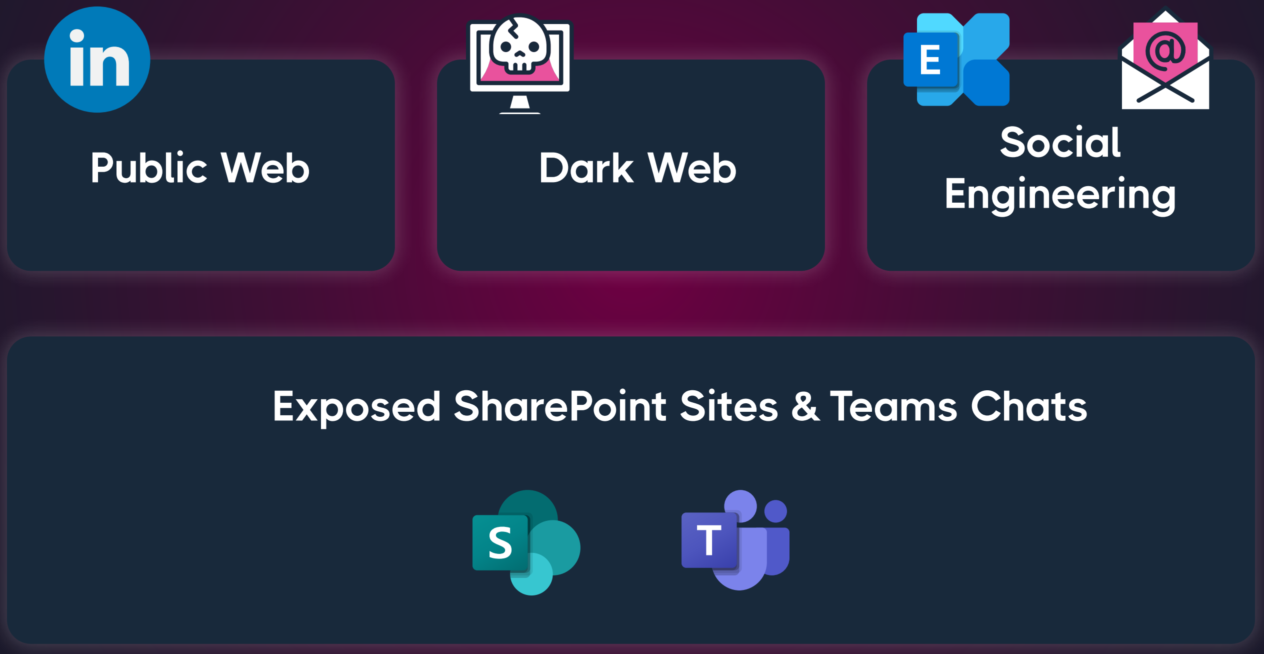
Many Microsoft 365 attacks will start with social engineering and spear phishing. For sophisticated attacks, cybercriminals will collect data online to build a picture of how an organization works to execute a compelling attack.

ACTION POINTS:

Prevention:

1. Train staff not to expose unnecessary information on LinkedIn and other related websites.
2. Create a standard template for work profiles with guidelines on what should and should not be included.

Reconnaissance



Public Web

Dark Web

Social Engineering

Exposed SharePoint Sites & Teams Chats

1(B): ADVANCED RECONNAISSANCE

PROBLEM:

If you have Teams chats or SharePoint sites that are exposed outside of your organization this not only creates a risk of sensitive data being exfiltrated but also creates a unique opportunity for research ahead of an attack. Social engineering will be more effective with this data.

As well as this, an existing threat within your business may configure external forwarding of mailboxes to ensure a steady stream of intelligence for further attacks.

ACTION POINTS:

Prevention/Detection:

1. Properly configure Microsoft's native DLP capabilities for Exchange, SharePoint, OneDrive, and Teams.
2. Monitor Microsoft's DLP configurations for configuration drift.
3. Continually detect Teams groups and SharePoint sites that are exposed to external users and have remediation processes in place to close these gaps.
4. Continually detect mailboxes that have been configured to auto-forward mail externally.
5. Train team members on suspicious email interactions and the need to safeguard sensitive organizational data.

Finding Exposed SharePoint Sites:

There are free tools online that allow anyone to scan your tenant for exposed SharePoint sites that can be targeted for reconnaissance. Here is how cyber criminals use them:

1. DNS Enumeration tools like "Sublist3r or Amass enable them to find relevant subdomains
2. Then a tool like Nmap enables them to identify SharePoint sites on these domains
3. Using "httpx" or "httprobe" they can then determine which subdomains are serving HTTP/s
4. And finally, looking through the relevant urls they can identify patterns indicative of a SharePoint site like /_vti_bin/

Finding Exposed Teams Groups:

Finding exposed Teams groups is more challenging than finding exposed SharePoint sites, but it is still possible. More and more organizations are using Teams for webinars, and some even share access to chats for public-facing work.

For example, marketing and community management teams may end up sharing access to Teams chats, which can lead to these being published in online forums and on the dark web.

Alternatively, advanced web-scraping tools may help attackers find ways into publicly exposed Teams chats.

1(C): DARK WEB RECONNAISSANCE & MARKETPLACES

PROBLEM:

In a research effort that identified more than 15 billion credentials in circulation on the dark web, Digital Shadows found domain admin accounts being auctioned for $120,000 on dark web marketplaces.

Cybercriminals can often bypass the early stages of the attack process by searching on the dark web to get ahead. Whether it is a powerful account or just some valuable intelligence, don't underestimate what they may find.

ACTION POINTS:

Prevention/Detection:

1. Enforce strong credential standards and multi-factor authentication for all Microsoft 365 accounts.
2. Work with 3rd parties to get an assessment of your dark web profile and risk exposure.

Part 2: **Entry**

2(A): BRUTE FORCE / PASSWORD SPRAYING

PROBLEM:

However unsophisticated a password spray attack may sound, the fact is that they remain extremely effective in the right circumstances.

When Midnight Blizzard breached Microsoft's environment, they did so with a classic password –spray technique which helped them identify exactly what they were looking for: a powerful account with a guessable password and no MFA.

ACTION POINTS:

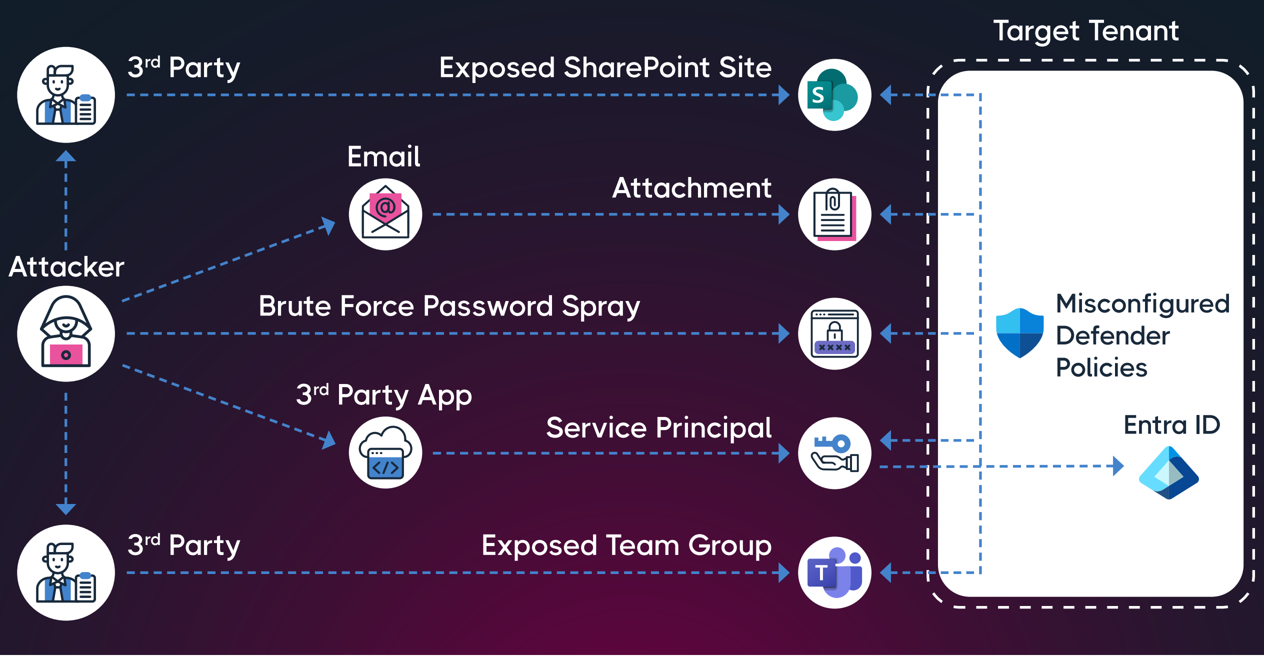
Prevention:

1. Enforce a strong password policy across all your Microsoft accounts.
2. Enforce MFA for all your Microsoft accounts.
3. Configure Conditional Access to block legacy authentication.
4. Ensure password protection is enabled for Entra ID.

Detection:

1. Report and alert on sudden spikes in failed logins.
2. Report and alert on high numbers of locked accounts.
3. Report and alert on unknown or invalid user attempts.

Different Ways an Attacker Could Break into a Tenant



2(B): EMAIL PHISHING & SPEAR PHISHING

PROBLEM:

No matter how sophisticated your email security is, you must allow normal human interactions to take place. This creates a window where spear-phishing can thrive.

Spear Phishing can have a wider variety of complex objectives, including ransomware deployment, financial fraud, and reconnaissance; but something to be especially conscious of is identity compromise.

Because Microsoft 365 has so many apps, configurations, and privileges to exploit, a cyber-criminal will often be satisfied to simply compromise a user account and get their hands dirty from within the tenant.

ACTION POINTS:

Prevention:

1. Ensure Microsoft Defender/ Advanced Threat Protection is properly configured.
2. Implement advanced email security beyond Microsoft's native Advanced Threat Protection capabilities.
3. Ensure the Safe Links policy is enabled.
4. Ensure internal phishing protection for Forms is enabled.
5. Ensure Microsoft Defender for Cloud Apps is enabled.
6. Ensure the spoofed domains report is reviewed weekly.
7. Run regular phishing simulation exercises and training for your teams.

Detection:

1. Monitor Microsoft Advanced Threat Protection for configuration drift.
2. Monitor Exchange for suspicious mailboxes, for example, mailboxes that have been set with external forwarding.
3. Enforce policies to detect anomalous account log-ins, for example, an account that typically logs in from a specific IP address/geo/device connects from somewhere different.

71% of Microsoft Office 365 deployments have suffered an account takeover of a legitimate user's account, not once, but on average seven times in the last year.

2(C): OAUTH CONSENT PHISHING

PROBLEM:

OAuth consent phishing tricks users into granting permissions to malicious apps that can access their data and perform actions on their behalf. Unlike traditional phishing that uses fake login pages, this attack uses legitimate OAuth 2.0 flows to deceive users.

These malicious apps request excessive permissions such as the ability to read emails or files. If executed correctly, the app gains access to their account data and can perform unauthorized actions without needing further interaction or passwords.

ACTION POINTS:

Prevention:

1. Configure Entra ID to require consent for 3rd party applications to get access to permissions.
2. Monitor Entra ID configurations to detect configuration drift.
3. Document a process for careful review of 3rd party application privileges.

Detection:

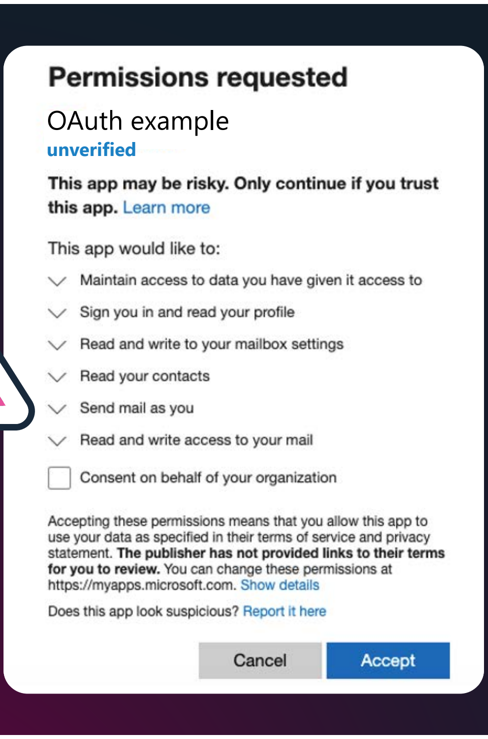
1. Enforce a process to detect 3rd party apps that are connecting to Entra ID and requiring excessive privilege.
2. Implement a process to have these apps reviewed and removed where appropriate.

Using OAuth Consent Phishing to access powerful Entra Privileges

Although less common than traditional phishing, these highly targeted attacks can be far more successful and sometimes hard to identify.

Cybercriminals conduct reconnaissance to understand which applications privileged users use or want to use. They then publish a third-party app and try to trick the user into approving access to it.

The App will request many powerful permissions, which the user will often approve. This will give the attacker immediate privileged access to your tenant through the app.



Permissions requested

OAuth example

unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read and write to your mailbox settings
- Read your contacts
- Send mail as you
- Read and write access to your mail

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

2(D): 3RD PARTIES & EXTERNAL USERS IN TEAMS & SHAREPOINT

PROBLEM:

Many organizations need to allow cross-tenant access to their Teams and SharePoint environments. This creates a channel that cybercriminals can exploit. The challenge is that you cannot enforce typical security policies on these accounts, like password complexity or MFA.

Despite this, they can still access sensitive SharePoint and OneDrive documents and be part of multiple M365 distribution and Teams groups, creating a unique window for attackers to leverage.

ACTION POINTS:

Prevention:

1. Create a governance plan that determines what external users can do, what data they can access, and what they can and cannot share.
2. Disable anonymous sharing, and limit external sharing of sensitive data.
3. Properly configure Microsoft's native DLP capabilities for Exchange, SharePoint, OneDrive, and Teams.
4. Monitor Microsoft's DLP configurations for configuration drift.

Detection:

1. Enforce a process to detect external users in Teams and SharePoint.
2. Enforce a process to identify public Teams groups.
3. Enforce a process to detect SharePoint sites with external sharing and no expiration policy.
4. Enforce a process to detect OneDrive files that are being share externally.
5. Enforce a lifecycle management process to decommission unused Teams and SharePoint sites.

2(E): PURCHASE PRIVILEGED M365 ACCOUNTS ON DARK WEB

PROBLEM:

In a research effort that identified more than 15 billion credentials in circulation on the dark web, Digital Shadows found domain admin accounts being auctioned for $120,000 on dark web marketplaces.

Cybercriminals can often bypass the early stages of the attack by searching the dark web to get ahead.

The challenge for Microsoft 365 users is often the tradeoff between having excess privilege and staying productive or restricting privilege and creating bottlenecks.

ACTION POINTS:

Prevention:

1. Compliance mandates like NIST, SOX, NIS, ASD, and others all require organizations to enforce Least Privilege, which is especially important for Microsoft 365. Global Admin and other privileged accounts give cybercriminals the power to destroy your business.
2. Try to delegate “just enough privilege” to administrators and regional teams. If you struggle with Microsoft’s delegation capabilities, seek a built-for-purpose solution to create least privilege access to your tenant.
3. Enforce strong credential standards for all Microsoft Online accounts.
4. Enforce MFA and a zero-trust approach for all logins.

Detection:

1. Work with 3rd parties to get an assessment of your dark web profile and risk exposure.

Microsoft Supply Chain Compromise

The true scale of the fallout from the Midnight Blizzard attack on Microsoft remains to be seen, but it is possible that Microsoft Cloud customers could experience supply chain attacks related to this initial breach.

Because of this, Microsoft Cloud customers must have best-practice security, governance, and oversight of their environments to detect and respond to any suspicious activity in their tenants.

Part 3: **Privilege Elevation**

Having gained entry to your environment, an attack will now typically focus on elevating their privileges and exploiting permissions so that they can more easily achieve their ultimate objectives.

3(A): USE COPILOT FOR INTERNAL RECONNAISSANCE

PROBLEM:

If an attacker compromises a standard user account that has a copilot license, they may be able to use copilot to quickly find valuable information.

As copilot is rolled out, many organizations are becoming aware that they have relied on “security by obscurity” in their Microsoft Cloud environments. Some files and pages have organization-wide sharing settings, meaning any user with Copilot could accidentally stumble on these files.

However, with Copilot for M365, there is a risk that anyone accessing a user account with a Copilot license can more quickly find important information that can help them plan the next stage of their attack.

ACTION POINTS:

Prevention:

Before Copilot for M365 is rolled out it is critical that organizations enforce strong governance across their collaboration environments:

1. Implement lifecycle management to decommission unused SharePoint and Teams environments, reducing the attack surface that must be managed.
2. Apply sensitivity labels in Purview Information Protection or configure restricted permissions in Information Rights Management (IRM) to restrict what Copilot for Microsoft 365 can access.

Detection:

1. Create reports to get visibility of who uses Copilot.
2. Put steps in place to prevent users from deleting their Copilot prompt history.

3(B): FIND/CREATE ENTRA APPS WITH EXCESS PERMISSIONS

PROBLEM:

When a user creates an application in Entra ID, it can easily be granted excessive permissions like the ability to fetch information about users in the directory, erasing messages from mailboxes, and sending emails.

Finding or creating an application with these privileges can give an attacker an easy pathway to elevate their access, much like what happened in the Midnight Blizzard Attack.

ACTION POINTS:

Prevention:

1. Put controls in place to restrict application registrations to specific users only.
2. Apply policy enforcement to detect and remediate dangerous Entra ID registrations.

Detection:

1. Report on Entra ID application registrations.
2. Report on Entra ID application permissions.

3(C): FIND 3RD PARTY APPS WITH EXCESS PERMISSIONS

PROBLEM:

Many 3rd party applications require Entra ID permissions for single sign on and other identity/ productivity enhancements. When they request these permission users rarely get good insight into what they are requesting and why.

Research from Adaptive Shield has shown that 67% of 3rd party apps request permissions that have medium to high levels of risks associated with them. 15% have privileges to read, create, update, and delete all the files you can access.

Large organizations can sometimes have over 1000 3rd party apps connecting to Entra ID, making this a highly effective target for cybercriminals.

ACTION POINTS:

Prevention:

1. Put controls in place to prevent 3rd party apps from being granted dangerous levels of privilege.
2. Apply policy enforcement to detect and remediate dangerous 3rd party apps.

Detection:

1. Report on 3rd party apps.
2. Report on 3rd party app permissions.

3(D): FIND POWERAPPS WITH EXCESS PERMISSIONS

PROBLEM:

The challenge of PowerApps parallels the Entra ID and 3rd Party App pains previously discussed.

Some organizations have taken advantage of the PowerApps capabilities included in their Microsoft ELA, only to later to realize there has been little governance over the creation and management of these apps.

This has led to many teams struggling with PowerApps sprawl, and, in some cases, permissions sprawl.

Quite often, PowerApps are not developed according to the principle of least privilege, meaning that there are apps in the tenant that could have useful permissions to be exploited.

ACTION POINTS:

Prevention:

1. Implement an internal governance strategy to manage and oversee PowerApps throughout their lifecycle
2. Ensure that security and governance stakeholders have input when PowerApps permissions are being configured.
3. Create a process to detect PowerApps with excessive permissions and trigger a remediation process to either decommission the app or reduce the permissions to an appropriate level.

Detection:

1. Report on PowerApps throughout your tenant
2. Report on PowerApps permissions throughout your tenant
3. Alert on newly created PowerApps with excessive permissions

3(E): FIND OR CREATE PRIVILEGED USER ACCOUNTS

PROBLEM:

Microsoft 365 has arguably the most powerful privileged account in an organization: The Global Admin account. The privileges associated with these accounts are so powerful that they can practically destroy a business under the right circumstances.

Microsoft does provide 80 different admin roles that are less privileged, but they are still far too powerful in many circumstances.

Despite the options that Microsoft provides, CoreView research has found that as many as 36% of Microsoft admins have used global admin privileges just to stay productive. This is because administrative teams are forced into choosing between security and productivity when working with Microsoft's native capabilities.

Compliance mandates like NIST, SOX, NIS, ASD, and others all require organizations to enforce Least Privilege, which is especially important for Microsoft 365.

There is a second level to this challenge too.

The onboarding process for a standard user account in Entra ID and Microsoft 365 is a tedious manual process. In mature organizations there can be as many as 50 manual steps for onboarding and another 50 for offboarding.

This is not only a drain of admin time, but also inevitably leads to misconfigurations and sometimes excessive permissions.

When All Else Fails...

Cybercriminals have multiple methods to easily obtain and exploit your personal information.

$60

for Personal Credit Card Details

On the Dark Web...

Cybercriminals can purchase privileged accounts to use on dark web auction sites.

$120,000

for a Domain Admin Account

ACTION POINTS:

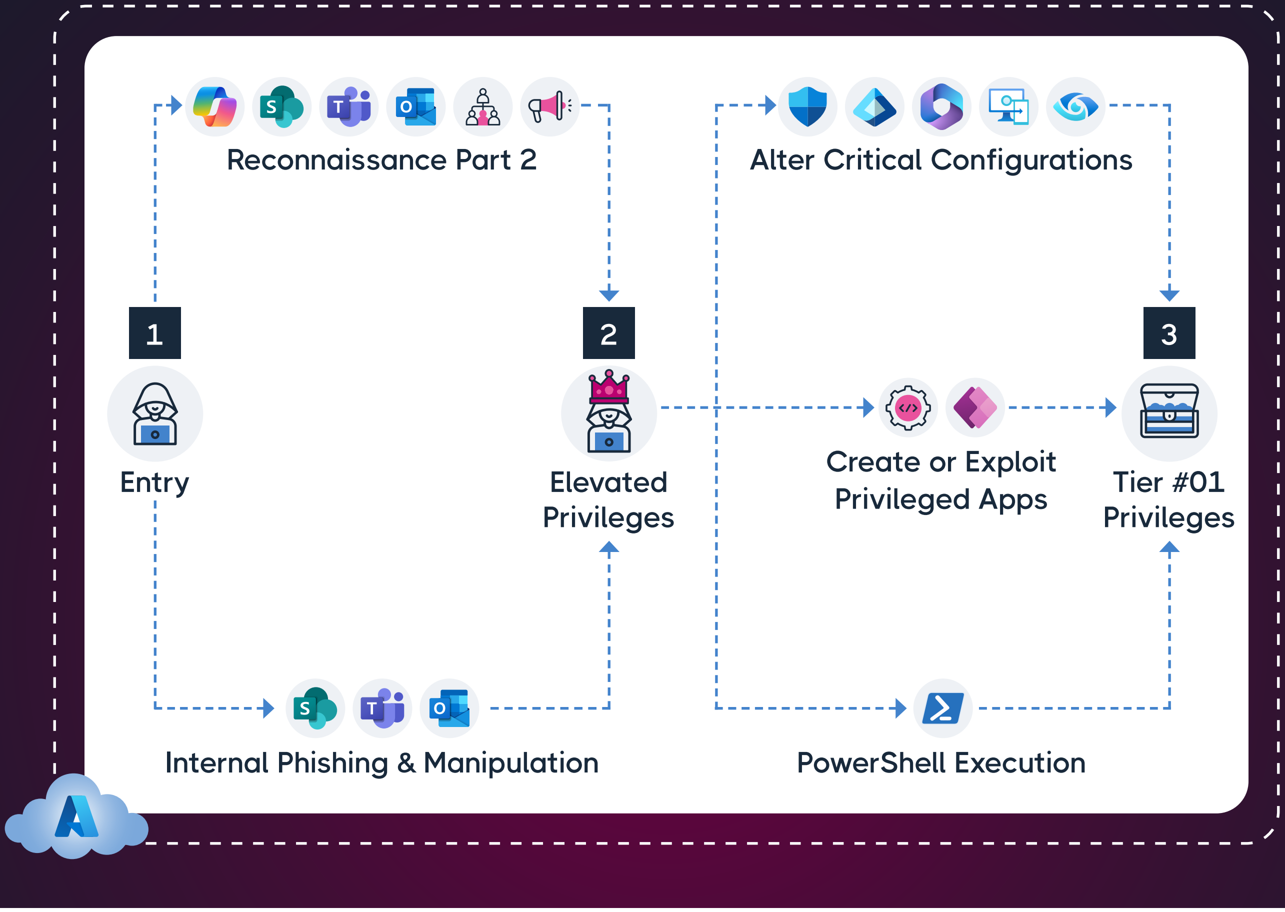
Prevention:

1. Leverage solutions to make it possible to delegate “just enough” access to administrators.
2. Enforce strong credential standards for all Microsoft Online accounts.
3. Enforce MFA and a zero-trust approach for all logins.
4. Monitor Entra ID and Purview Privilege Management for configuration changes.
5. Automate the user onboarding and offboarding process to avoid misconfigured permissions for users.

Detection:

1. Monitor Entra ID and Purview Privilege Management for configuration changes.
2. Get alerts for suspicious log ins.

What Happens When an Attacker Gains Entry


Reconnaissance Part 2
Alter Critical Configurations
1
Entry
2
Elevated Privileges
Create or Exploit Privileged Apps
3
Tier #01 Privileges
Internal Phishing & Manipulation
PowerShell Execution

3(F): POWERSHELL & COMMAND EXECUTION

PROBLEM:

Scripting opens huge productivity for administrations, but it also gives attackers a rapid way to make progress in your environment.

Adversaries may abuse command and PowerShell for information gathering and to launch remote scripts to machines.

These may also be used to discover how permissions are configured and where best to focus their attack for privilege elevation.

ACTION POINTS:

Prevention:

1. Use PowerShell constrained language mode to restrict access to dangerous language elements.
2. Restrict PowerShell execution to administrators.
3. Use PowerShell JEA “Just Enough Administration” to limit what commands admins and users can run.

Detection:

1. Monitor PowerShell script execution and subsequent behaviors.
2. Monitor log files for process execution.

Part 4: Persistence & Evasion

Now that the attacker has the power they desire, their next concern is to ensure they cannot easily be removed.

4(A): CHANGE SECURITY SETTINGS

PROBLEM:

Microsoft 365 has over 5000 configurations. Large organizations with complex environments can have hundreds of thousands or millions of specific configurations in their tenant.

Monitoring these configurations to ensure they are not being changed (or "drifting") is practically impossible at scale, making it easy for cybercriminals with the right privileges to start playing with Entra ID, Defender, Intune, and Purview to start opening more windows for further attacks.

Changing configurations like conditional access policies, external identity management, cross-tenant access, authentication, DLP, and ATP threat management configurations could leave a window open to allow an attacker easy access back into your environment if they are detected.

ACTION POINTS:

Prevention:

1. Microsoft, NIST, CIS, HIPAA, and others all now recommend that organizations implement "robust configuration change management" to ensure that configuration changes are all tested to avoid misconfigurations that can be exploited.
2. Use tenant configuration management capabilities to template your ideal configurations and auto-deploy them with consistency across your tenants.
3. Use configuration management capabilities to detect when configurations drift and roll them back to your ideal state.

Detection:

1. Use tenant configuration management capabilities to detect when configurations drift and roll them back to your ideal state.

4(B): CREATE NEW APPS & ACCOUNTS

PROBLEM:

In the Midnight Blizzard attack, cybercriminals found a highly privileged OAUTH app to exploit, and then immediately created new OAUTH applications in the tenant that would ensure they had continued access to the privileges they needed, even if the initial OAUTH application was suddenly decommissioned.

ACTION POINTS:

Prevention:

1. Put controls in place to prevent dangerous application registrations.
2. Apply policy enforcement to detect and remediate dangerous Entra ID registrations.

Detection:

1. Monitor your tenants for configuration changes.
2. Report on Entra ID application registrations.
3. Report on Entra ID application permissions.

4(C): DELETE AUDIT LOGS AND HIDE ARTIFACTS

PROBLEM:

In an effort to prevent detection, adversaries may disrupt audit logging or try to hide artifacts like privileged accounts and applications they have created.

Microsoft Purview's unified audit logging and defender for cloud apps UEBA are likely to be targets for this kind of activity.

ACTION POINTS:

Prevention:

1. Monitor your tenants for configuration changes in Purview and Defender for Cloud Apps.
2. Implement configuration change management to ensure that misconfigurations don't make it into production tenants.

Detection:

1. Monitor your tenants for configuration changes in Purview and Defender for Cloud Apps.

4(D): MONITOR EMAIL & SET UP AUTO-FORWARDING

PROBLEM:

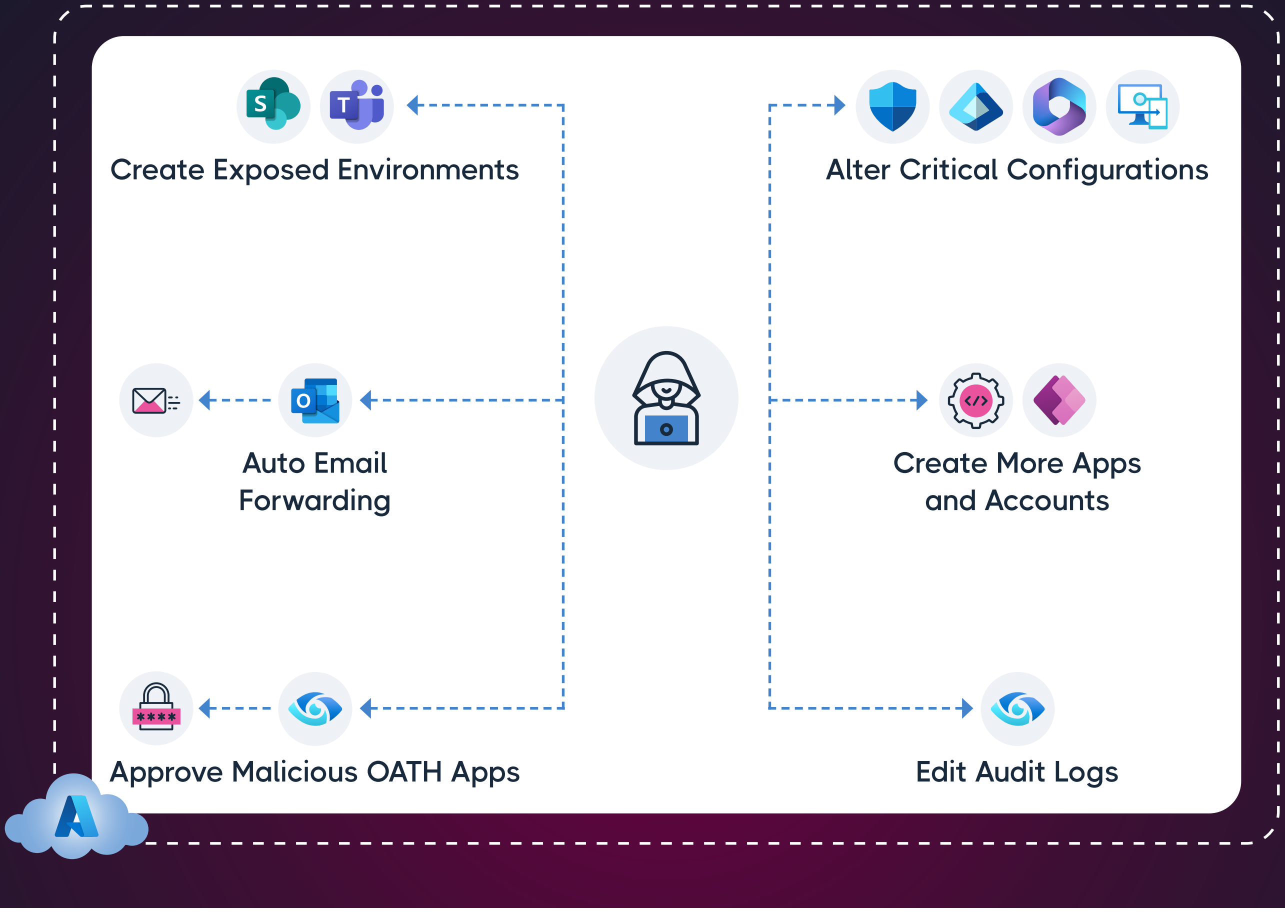
For those seeking to maintain a long-term presence, compromising and exploiting mailboxes is a valuable strategy. Cybercriminals who have compromised a mailbox can set up rules to hide their impersonated communications with colleagues, turn off audit and litigation hold to hinder investigation of activity, and set up auto-forwarding to ensure they continue to get access to valuable communications.

ACTION POINTS:

Prevention:

1. Report and alert on mailboxes without audit or litigation hold.
2. Report and alert on mailboxes with auto-forwarding.
3. Report and alert on exchange activity to detect anomalies.

Strategies for Persistence and Elevation


Create Exposed Environments
Alter Critical Configurations
Auto Email Forwarding
Create More Apps and Accounts
Approve Malicious OATH Apps
Edit Audit Logs

Part 5: Ransom, Exfiltration, & Disaster

With their powers secured, the attacker will now push to achieve their aim. This can vary dramatically based on the motivations of the attacker.

5(A): ENCRYPT TENANT AND HOLD BUSINESS TO RANSOM

PROBLEM:

It's becoming increasingly common for cybercriminals to target an organization's tenant in their ransomware strategy.

Given that Microsoft 365 customers often rely on Teams, Exchange, Entra ID, and SharePoint as the foundation of their digital workspace, it makes complete sense that it has become a priority target.

In these scenarios, organizations often need to be able to rapidly rebuild their tenant to get their business operations back to normal and to minimize expensive downtime and reputational damage.

However, Microsoft does not provide a native capability to back up and restore Microsoft 365 configurations.

ACTION POINTS:

Prevention:

1. Configure Microsoft Defender/Advanced Threat Protection to protect against suspicious links, attachments, and other payloads for ransomware.
2. Configure Defender for Cloud Apps to defend against web-based attacks.
3. Ensure users are trained on how to detect suspicious emails and to respond appropriately.
4. Regularly back-up tenant data and configurations so you can quickly rebuild a tenant in a disaster scenario.

5(B): EXFILTRATION OF SENSITIVE DATA

PROBLEM:

In some instances, an attacker will simply be searching for sensitive data for their own purposes, or to sell on the dark web.

In these circumstances, once the data has been identified it will need to be exfiltrated. In some cases, the data will be minimal, making the exfiltration easy and practically undetectable. For example, if they were just looking for privileged accounts to auction on the dark web, they could easily save these credentials in a variety of ways.

However, when there is a large volume of data, they will need to be more sophisticated in their activities to avoid triggering Microsoft's Behavioral Analytics

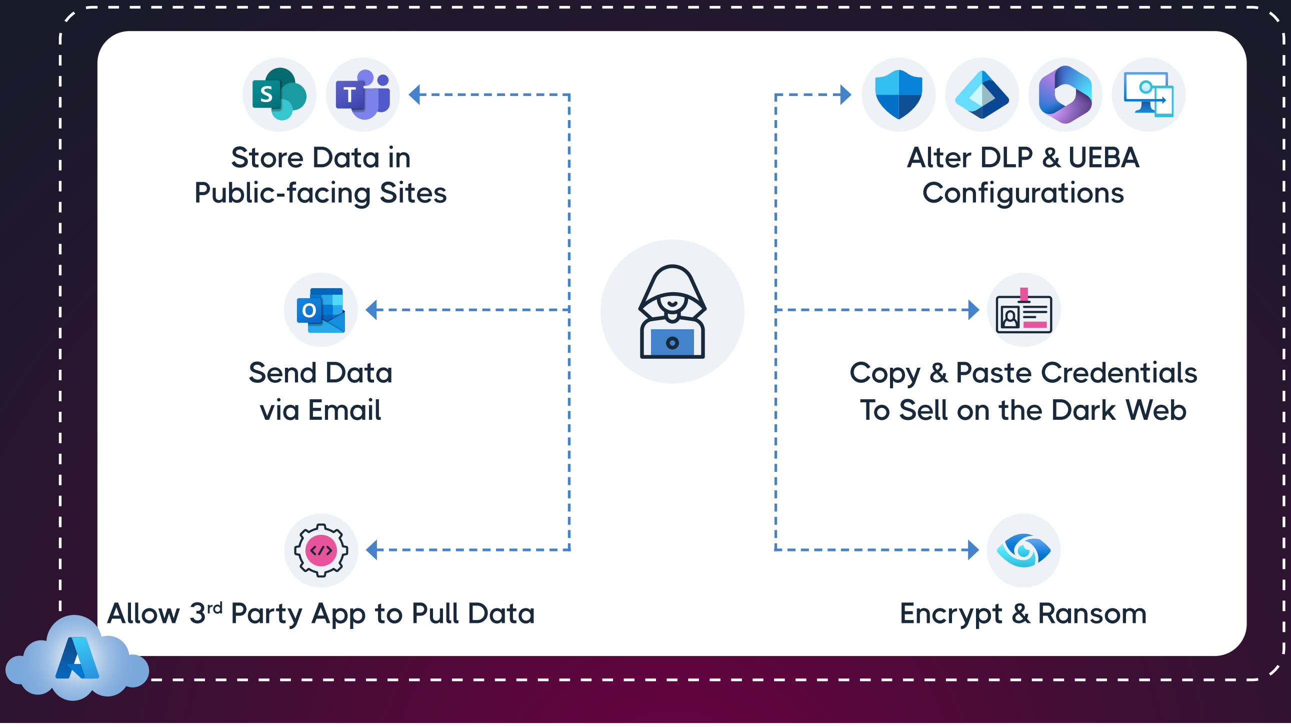
Some approaches include the use of webhooks, command prompts, backup and sync operations, and email.

ACTION POINTS:

Prevention:

1. Properly configure UEBA/DLP.
2. Monitor email for suspicious activity.

Data Exfiltration & Disaster


Store Data in Public-facing Sites
Send Data via Email
Allow 3rd Party App to Pull Data
Alter DLP & UEBA Configurations
Copy & Paste Credentials To Sell on the Dark Web
Encrypt & Ransom

The Easier Way to Secure Microsoft 365

Now that we've explored the dangerous vulnerabilities and attack vectors in Microsoft 365, it's clear that securing this vital infrastructure is a monumental task. The sheer scale and intricacy of the Microsoft 365 ecosystem can make it seem like an insurmountable challenge. But it doesn't have to be.

With CoreView, you can drastically improve your Microsoft 365 security posture—without sacrificing productivity. Our comprehensive platform lets you continuously monitor configurations, detect anomalies, and respond proactively to any indications of attack. This ensures risks are mitigated before they develop into full-blown breaches.

Automated Policy Enforcement

Continuously monitor all your critical workloads so your team can focus on higher-value strategic initiatives.

Configuration Management

Back up tenant configurations and detect drift to prevent misconfigurations and maintain desired states.

Delegated Administration

Grant "just enough" access to users to minimize overprivileged accounts without sacrificing productivity.

READY TO GET STARTED?

Entra App Security Scanner: Download this free tool to find custom and third-party apps with unauthorized access and overprivileged permissions.

Discover and Secure Your Apps Now

Admin Permissions Scanner for Microsoft 365: 57% of organizations have overprivileged admins—is your tenant vulnerable? Use this tool to find and fix your M365 admins with too much access.

Protect Your Tenant—Scan Your Permissions Today

See CoreView in Action: Learn how to deliver best practice Security, Governance, and Administration for Microsoft 365 with CoreView.

Explore CoreView Solutions Now

Authors and Key Contributors

Vasil Michev

Michev is a 9-time Microsoft MVP whose Microsoft 365 expertise covers all stages of the lifecycle: planning, POC and pilot, migration, adoption/training, security, and ongoing support.

Terence Jackson

Jackson is a seasoned leader in cybersecurity and IT with over 20 years of experience. He specializes in breach analysis and security solutions, serving as Microsoft's Chief Customer Security Officer.

Rob Edmondson

Edmondson is a leading expert with a decade of experience in Microsoft 365, DevOps, and Identity Security, specializing in email security and privileged access management in the SaaS space.

Sharon Breeze

Breeze has over 25 years of experience in Microsoft and IT. Starting as a Computing Officer, she has held technical roles at major tech companies like Fujitsu and Hewlett-Packard.

ABOUT COREVIEW

CoreView is the Global Leader in Effortless M365 Security, Governance, and Administration. Offering an end-to-end solution that stretches across the whole M365 ecosystem; from your tenant level configurations, right up to your most critical workloads.

Created by M365 experts, for M365 experts, CoreView makes best practice for M365 effortless by simplifying, unifying, and enhancing the M365 admin experience. CoreView empowers 1500 M365 organizations to turn the tide on endless tasks, deliver best practice security, and drive ROI.