Office Under Siege

Understanding, Discovering, and Preventing Attacks Against M365

DMITRIY BERYOZA

Slides can be found at https://github.com/0xd13a/presentations

About me

Dmitriy Beryoza

@0xd13a on Discord/Twitter

https://www.linkedin.com/in/beryozad

VECTRA®

- Senior Security Researcher at *Vectra AI*
- Prior to that - Pentester/Secure Software Development Advocate with X-Force Ethical Hacking Team at *IBM Security*
- 25+ years in software design and development
- Ph.D. in Computer Science, CEH, OSCP, CISSP, CCSP
- *Interests*: reverse engineering, secure software development, CTFs

Agenda

- Introduction to M365
- Security Expectations in the Cloud
- Recent Incidents
- Popular Attack Techniques
- Defender Tools
- Defense Strategies

Introduction to M365

What is Microsoft 365?

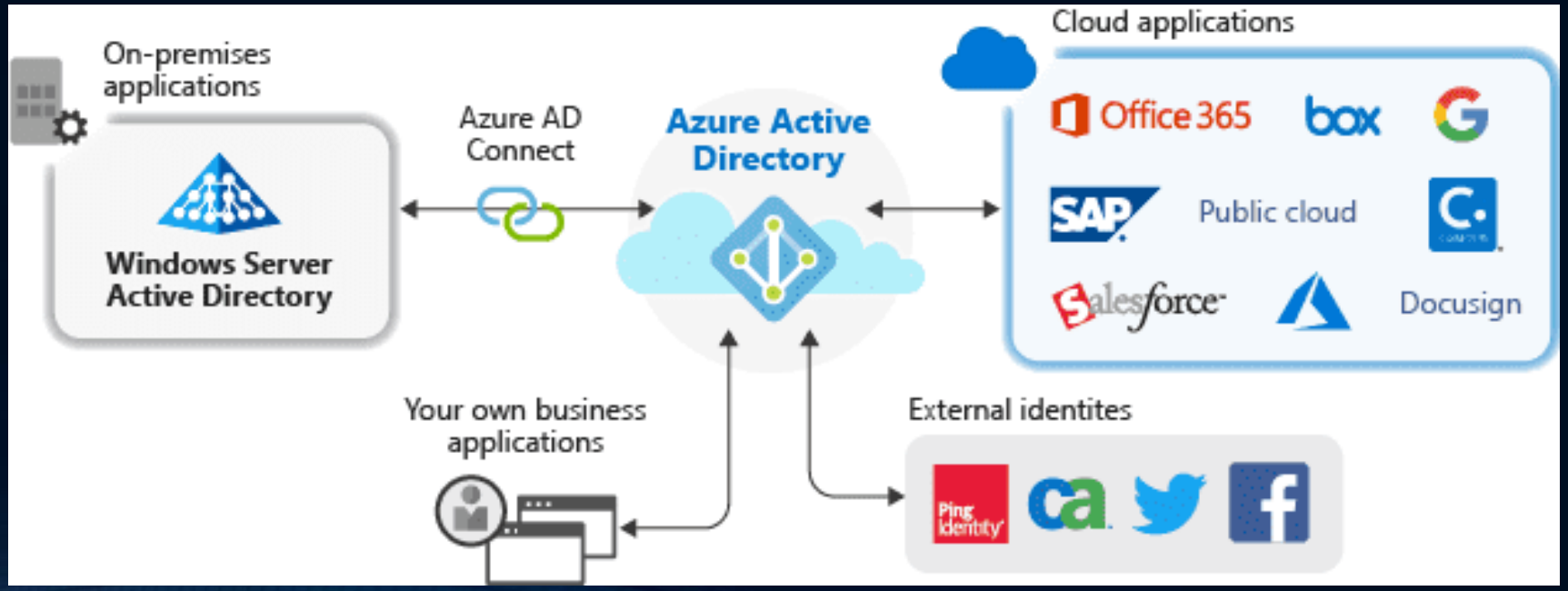
Microsoft 365

- Formerly Office 365/O365 (launched in 2010)
- Line of productivity SaaS ("Software as a Service") subscription services
  - Cloud-based MS Office
  - Teams, Exchange Online, Skype, SharePoint, OneDrive, …
- 300M+ monthly active users, 2M+ organizations
- >60% users - small businesses (<50 employees)
- ~48% of global office suite market (Feb 2022)

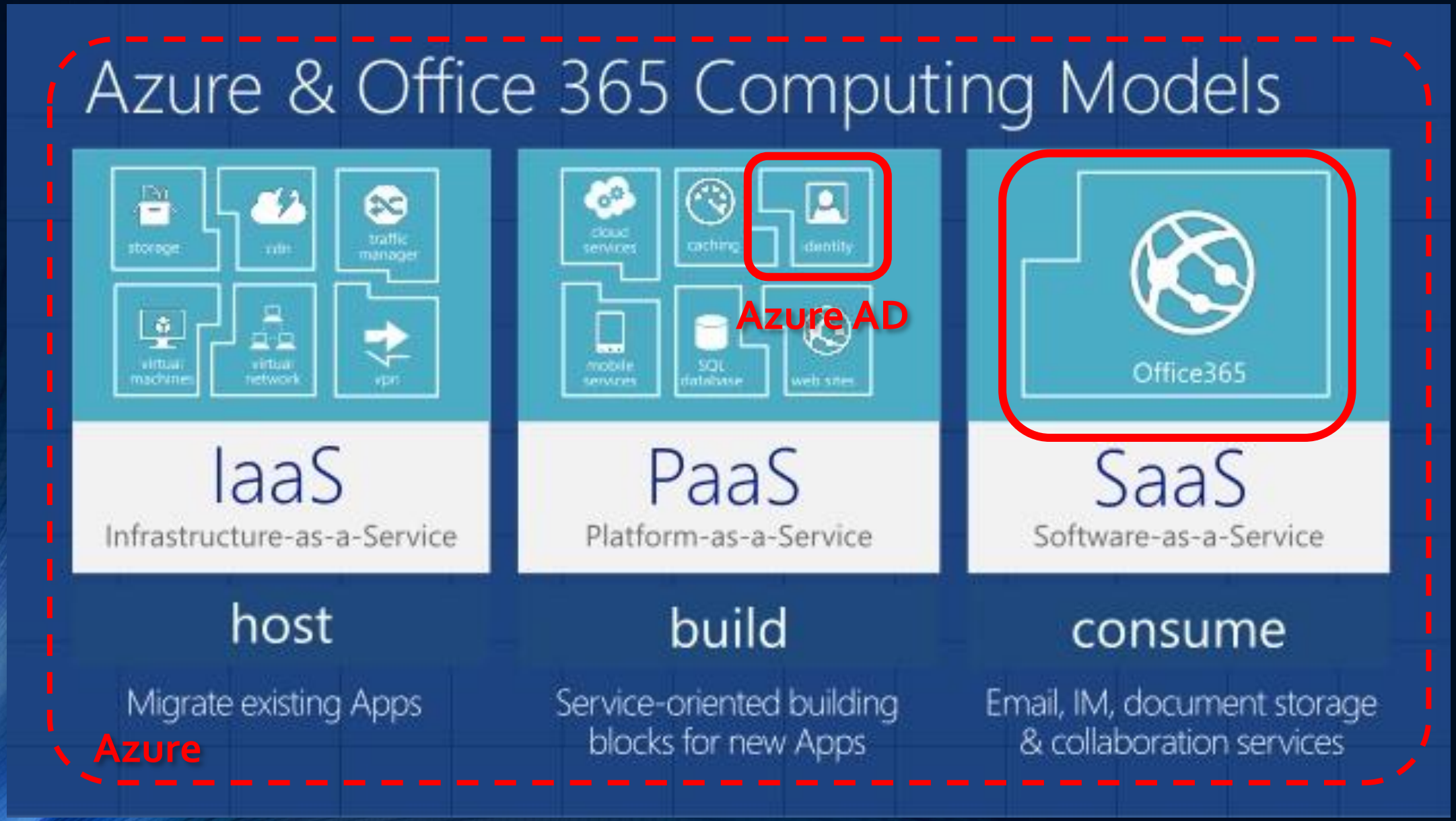
Azure AD

Azure AD

- It's impossible to talk about M365 security without also talking about Azure AD
- Cloud-based directory and identity management service (*differs from Active Directory*)
- In our context - provides *authentication* and *authorization* for M365 users
- Allows users to sign up for services and access them with a single set of credentials
- Provides access to cloud and on prem apps
- Supports modern authentication, AD synching, federation, device management, etc.
- Integrates with other identity providers (e.g. Okta)
- 425M daily active users (Jan 2021)



M365 and AAD in Azure Ecosystem



Why Does Security of M365 Matter?

- What's there to steal?
- M365 is a treasure trove for the attacker:
  - Corporate documents and data on SharePoint and OneDrive, sometimes including IT blueprints and passwords
  - Corporate e-mail with data on finances, accounts, credentials
  - Teams chats where sensitive data is often shared
- Opportunities for:
  - Sensitive data collection and exfil (with extortion opportunities)
  - Impersonation leading to lateral movement, spear-phishing, and whaling
  - Command and Control (C2)
  - Pivot into other SaaS, cloud, and on-prem environments

Security Expectations in the Cloud

Securing the Cloud

- Cloud comes with a promise of better security
  - Overall, it does hold true, security is improved
  - Many attack scenarios that are plaguing the on-prem environments are eliminated
    - But new weak points can be introduced; "the devil is in the details"
- *ProxyShell* family of vulnerabilities is a good example
  - Unpatched instances of Exchange are still vulnerable in many customer environments
    - …and will be vulnerable for a long time
  - M365 Exchange Online functionality (if it was vulnerable) was likely patched before the bugs were announced
- Cloud provider, however, does not promise to secure "everything"
  - Rather, a "Shared Responsibility Model" is used

Shared Responsibility Model

- Customer is responsible for securing the configuration, provider - for the security of software and infrastructure

Defending M365/AAD - The Good

- Infrastructure secured and patched across the board
  - 0days have very limited shelf life, often fixed before being announced or shortly after discovery in the wild
  - ***Most attacks are against the configuration***
- Uniform APIs across many customers
  - Better understood and tested
- Specialization promotes better security
  - Cloud providers and vendors specialize in defending and configuring the cloud
- Cloud providers have visibility into customer environments
  - Can spot and help fix problems at scale
  - Richer log events are available
- Relatively new
  - Attackers are still learning how to exploit it
  - Catalog of attack methods is much smaller than for classic attacks
- Obscurity helps security - code is private

Defending M365/AAD - The Not So Good

- Relatively new - defenders still need to learn how to secure it properly
- Wide open attack surface
  - Sometimes compromising the identity is all that's needed
- Configuration mechanisms are at times hard to understand and use correctly
- Built-in admin and monitoring tools not perfect, have blind spots
- Visibility limited to signal in the logs, which have their own issues (discussed later)
- Some security features depend on expensive subscription levels

Under Attack

Attack Trends

- M365/AAD attacks are steadily increasing
  - Not necessarily because SaaS is easy to exploit
  - Attackers just follow the assets and the money
- COVID-19 put migration to the cloud into overdrive
  - Azure AD helps secure a multitude of online services
  - M365 is the leader in the cloud-based office and productivity application market
  - As a result of increased migration attacks grew at an even faster pace
- **By some estimates in the past 2 years there were 300K+ attacks of all sizes**

High Profile Attacks

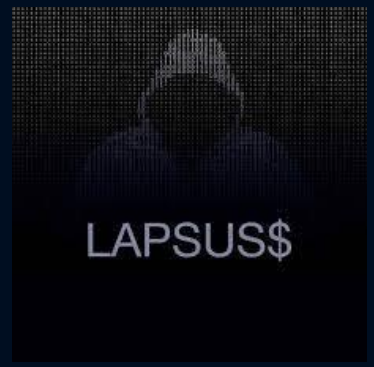
UNC2452/Dark Halo - "Sunburst"

- Large-scale intelligence gathering operation affecting > 200 orgs (US Gov. agencies, Microsoft, FireEye, and others)
- Primarily on-prem, but included a cloud portion

- *Golden SAML Attack* - compromised on-prem AD to mint their own SAML tokens, allowing sign-ins bypassing MFA
- *Modification of Trusted Domains* - added their own domain as federated, or modified existing one, to get user automatically trusted by the victim domain
- *Abuse of Mailbox Folder Permissions* - granted compromised low-level user read permission on target mailboxes
- *Hijacking of Azure AD Application* - access to existing application backdoored to execute privileged actions

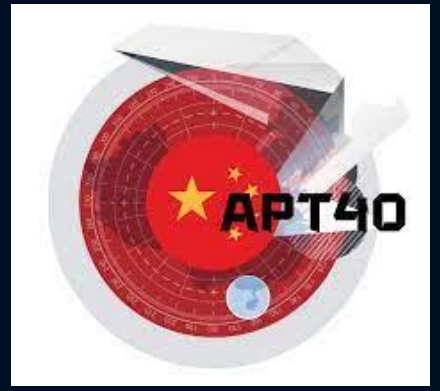
High Profile Attacks (continued)

Lapsus$



- Breached Microsoft, Nvidia, Samsung, Okta, and others
- Upon breaching a cloud tenant *created a new Global Admin account and deleted all others* to restrict access
- Set an Office 365 *tenant level mail transport rule* to send all mail in and out of the organization to the newly-created account

APT40/Kryptonite Panda

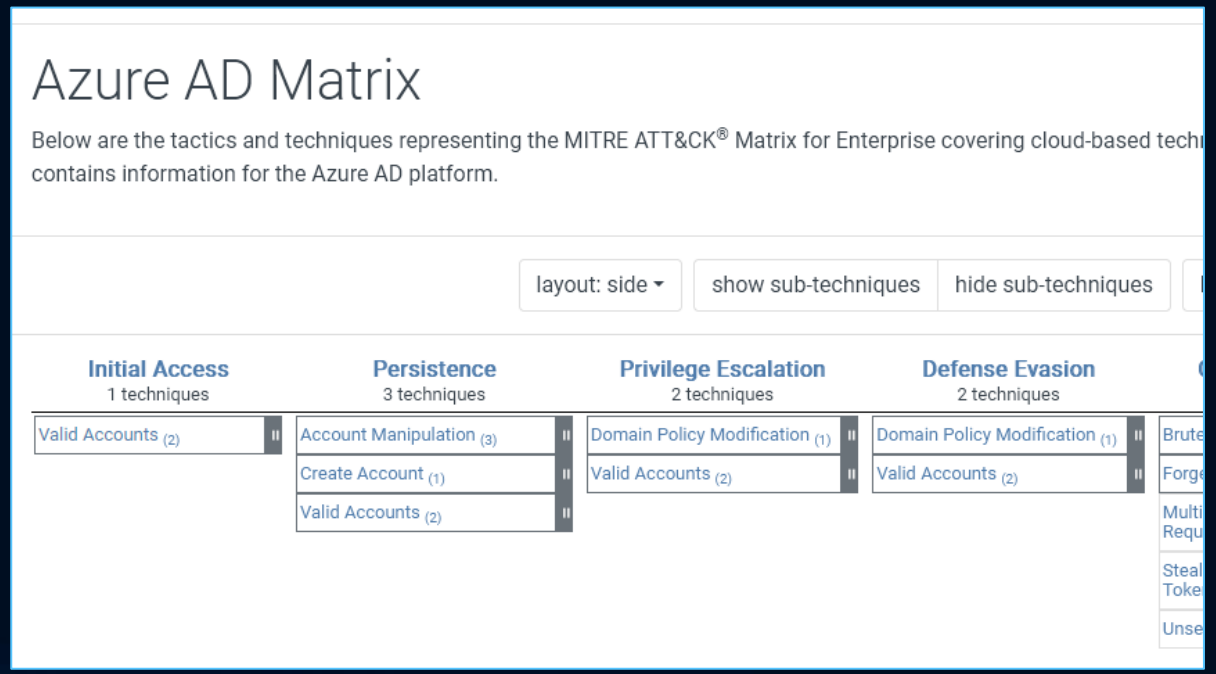


- Started with malicious attachments in phishing e-mails
- Connected to Outlook Tasks, Outlook Contacts and OneDrive APIs for *C2 communications* and *file download/exfil*
- Configured *malicious app with OneDrive permissions*
- Used OneDrive to *convey commands, download other exploitation stages,* and *store exfiltrated files*

Attack Techniques

MITRE ATT&CK for Cloud

- MITRE ATT&CK for Cloud is a good resource for enumerating different attacks types
- MITRE provides matrices for AAD and M365: https://attack.mitre.org/matrices/enterprise/cloud/



Password Attacks

- Various types of bruteforcing are seen in M365/AAD
- Microsoft has measures in place to detect and mitigate most obvious exploits (e.g., with auto account lockout)
- To make sign-in attempts look natural smart attackers use:
  - *Delays* to space attacks out in time
  - *Jitter* to make them look less automatic
  - *VPNs/TOR/proxies* in order to imitate logins from random locations, or the same geo as the valid user
- For a multiple accounts attackers will use *password spraying*
  - *"Try the 1st password across the entire set of users, then the 2nd, and so on"*
  - This extends the time between login attempts for each user, fooling the defenses

MFA Will Save the Day?

- Enabling MFA is the best defense against password exploitation
  - But there are ways attackers will try to bypass it
- Popular tactics:
  - *Attacker in the Middle (AitM)* - phishing user to with a fake login front and forwarding all the answers to the legitimate login prompt
  - *MFA Fatigue* - "annoying" user into authorizing the sign-in by bombarding them with push prompts
- More ways to bypass MFA:
  - Intercept or social engineer SMS codes
  - Steal a cookie with satisfied MFA claim
  - Abuse legacy APIs (e.g., POP3 and IMAP) that cannot work with MFA
  - Disable MFA altogether if privileged access is acquired
  - Change trusted network settings to selectively avoid MFA prompting

Phishing

- Phishing is another favorite initial access vector
  - Malicious malware attachments
  - Links to web sites that drop malware or exploit browser vulns
  - Links to fake login fronts
- Various types of phishing are observed
  - *Regular phishing* casts a wide net in the hopes of compromising arbitrary accounts
  - *Spear phishing* is directed against select groups of people, such as management and IT, for privilege escalation
  - *Whaling* is done in sophisticated BEC schemes to trick executives into authorizing significant money transfers
- Once victim has malware dropped on their machine or gives up their credentials, further exploitation is done to establish persistency and move laterally

Abuse of Trusted Relationships

- M365 and AAD security sometimes relies on external mechanisms for authorizing access to the environment
- *Federated relationships*
  - AAD lets customer set up a trust relationship with another domain
  - If attacker gains privileges, they can add a malicious domain relationship to have access to the target without preconditions
- *Golden SAML*
  - This technique is made possible by a compromise of an on-prem AD that synchs with AAD
  - Attacker can forge their own authentication tokens for easy access to the cloud environment
- *Session cookie theft*
  - Malware on the user device may steal browser cookie for the open session
  - It is then used on attacker's machine to gain access

Persistent Access

- After the initial compromise one of the first thing the attackers often do is establish multiple redundant ways to get into the system

- Persistence can be achieved through:
  - Creation of new accounts with elevated privileges
  - Granting new powers to existing accounts
  - Adding redundant keys or additional MFA factors to existing accounts
  - Abuse of Service Principals (automated accounts that are low key yet can have admin powers)
  - Tricking users into giving malicious apps permission to impersonate them (*OAuth consent grant*)

Recon

- Account enumeration
  - User accounts can be discovered through sign-in attempts (via error codes)
  - Attackers sometimes try first/last names combinations and permutations

- **Unfortunately, in M365/AAD we are blind to most recon activity**
  - Azure does not log majority of requests that read configuration, enumerate users, groups, resources, etc.
  - Once attacker gains access to the tenant, requests to map available resources will not trigger security alerts

Disabling of Security Mechanisms

- With multiple security mechanisms available, the particularly stealthy way to bypass some of them is to disable them rather than try to break them
- Logging gives customers the primary way of monitoring what is going on in the environment
  - Disabling it blinds defenders to any subsequent malicious activity
- Conditional access rules may deny access from some locations, and may add more stringent rules for signing in from others
  - They can be relaxed or disabled in order to simplify access from a specific malicious machine
- Built in protections against phishing, malware, malicious URLs help protect users from social engineering attacks
  - Disabling them opens the door to wider account compromise within the company
- Many other security settings can be adjusted slightly to blind the blue team to specific types of attacks

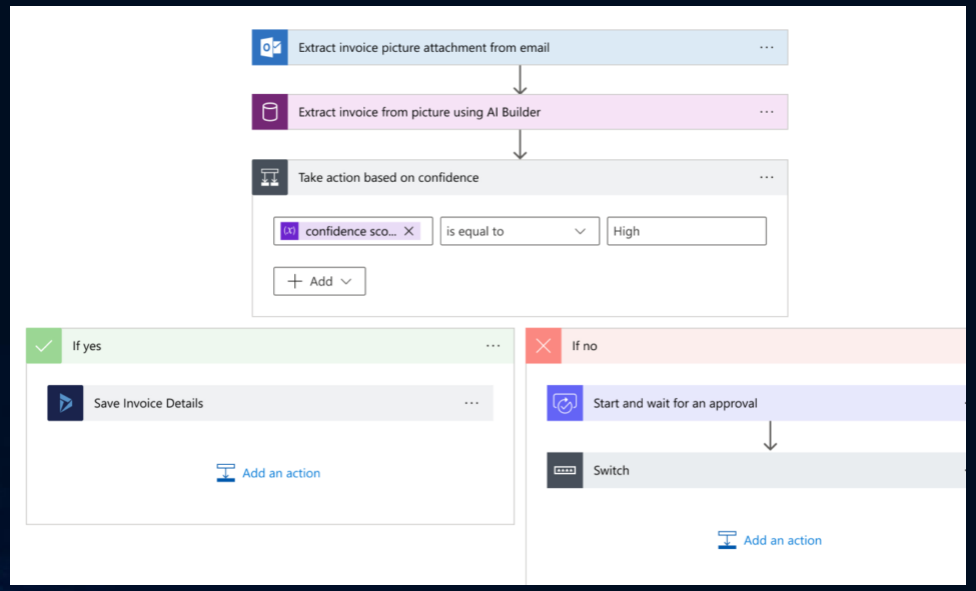
Malicious E-mail Rules

- Facilitate internal spear phishing, whaling, and BEC scams.
- A popular post-exploitation step
- Emails are hidden (by redirecting them to an unusual folder: e.g., *RSS Subscriptions*, *Notes*, or others), or deleted
  - Victim should be made unaware of e-mails sent on their behalf and subsequent responses to them
- Emails are redirected to external location for exfiltration
- Selection criteria are often the giveaway: keywords such as "hack", "scam", "payment", "wire"

```
[
    {"name":"AlwaysDeleteOutlookRulesBlob", "value":"False"},
    {"name":"Force", "value":"False"},
    {"name":"Name", "value":"."},
    {"name":"SubjectOrBodyContainsWords",
        "value":"spam;hacked;suspicious link;compromised;phishing;bitcoin"},
    {"name":"DeleteMessage", "value":"True"},
    {"name":"StopProcessingRules", "value":"True"}
]
```

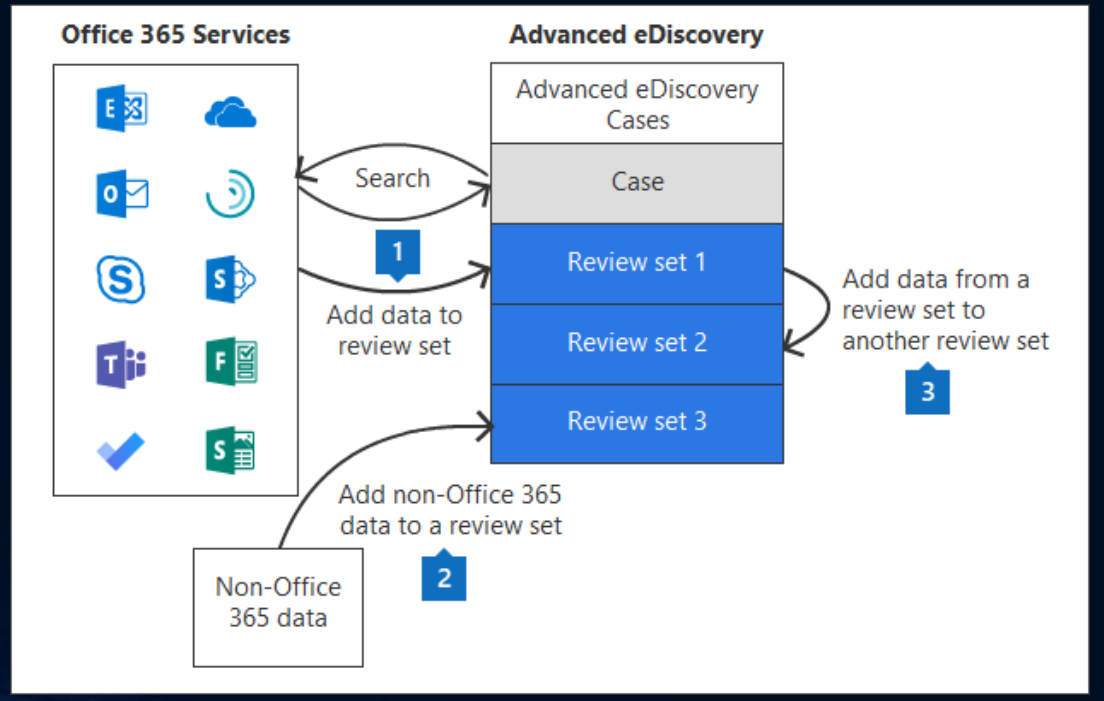
Abuse of Power Automate

- *Power Automate* - low-code automation functionality available in M365
- Visual programming by combining "connectors", which represent:
  - Program flow control (variables, "if" statements, loops)
  - Services (SharePoint, Teams, Exchange, Twitter, Facebook, etc.)
- Many useful scenarios covered: email sorting, backups, triggering of jobs
- In malicious cases could be used to build covert C2 servers:
  - Receive, and respond to HTTP requests
  - Download malware
  - Exfiltrate data



Abuse of eDiscovery

- Service built to assist in legal investigations and evidence collection
- Holds unusual amount of power over all user data
  - One can use it to search and copy data from arbitrary files, chat transcripts, emails
  - Essentially "super user"-like visibility into all data in the organization
  - Can be abused for stealing business secrets, passwords, keys, etc.
- Attacker would compromise the user with eDiscovery powers to take advantage of this functionality



Data Collection and Exfiltration

- *OneDrive* and *SharePoint* represent convenient vehicles for:
  - Accumulating stolen data
  - Making it available for exfiltration
  - Sharing malicious content
- Data that is collected can be shared anonymously, not requiring an account to download it
- *Exchange mailboxes* can be modified for anonymous external access or access by a low-level user
  - Attacker can then connect periodically and download relevant e-mails
- *Microsoft Teams* allows guest access for external users
  - Malicious user could get an invitation through social engineering
  - Proprietary information appearing in the team channels can then be collected

Ransomware

- *Ransomware risks seem lower in M365 and AAD than in traditional environments*
- Encryption of SharePoint and OneDrive data is possible but built-in versioning mechanisms allow rollback
  - Researchers proposed reducing max version numbers to bypass this
- Attackers have been observed in the past deleting and locking out Global Admin accounts, but Microsoft support has the power to override that
- In-place encryption of e-mails in Exchange was demonstrated by Mitnick (https://www.youtube.com/watch?v=VX59Gf-Twwo) but not yet seen in the wild
- *Customer Key (or BYOK)* setup may allow ransomware
  - Customer with strict privacy needs may configure their own M365 data encryption keys
  - If attacker acquires privileges to "rotate" keys, they could hold data for ransom

Defender's Toolbox

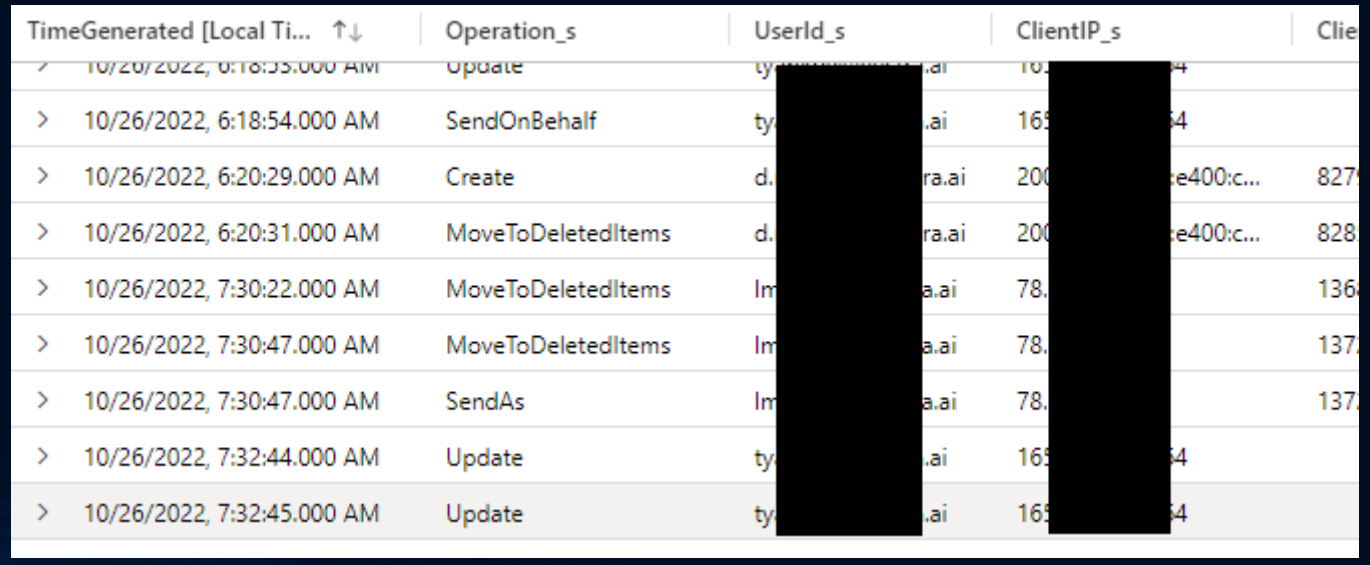
Defense Tools

- A variety of security mechanisms are built into M365/AAD (groups, roles, security settings, etc.)
- Microsoft 365 Defender
  - Spam and phishing protection, safe attachments and links, and more
- Microsoft Sentinel - native SIEM solution, ingests logs from variety of sources
  - Has a variety of built-in detections and allows you to define your own
- Azure Log Analytics - powerful log analysis platform, Kusto query language
  - Good for ad-hoc investigations for security events
- 3rd party tools add value in posture management and malicious behavior detection

```
StormEvents
| where StartTime between (datetime(2007-11-01) .. datetime(2007-12-01))
| where State == "FLORIDA"
| count
```

Logs

- Azure logs provide the only view into what is happening in M365/AAD environment
  - More telemetry is visible to Microsoft, but not shared with the customers
- Available logs:
  - Graph API: *Signins (*multiple flavors covering *interactive, noninteractive, managed identities, etc.),* and *Directory Audits*
  - O365 Management API: *AuditAzureActiveDirectory*, *AuditGeneral*, *AuditExchange*, *AuditSharepoint*, *DlpAll*
  - There is some overlap between the information provided by the 2 APIs
- Common information available:
  - Timestamp
  - Actor info (user, IP, device, OS, browser, geolocation)
  - Target (service, resource)
  - Operation name and details
  - Result status and error details



TimeGenerated [Local Ti...	Operation_s	UserId_s	ClientIP_s	Clie
10/26/2022, 6:18:54.000 AM	SendOnBehalf	[redacted]	[redacted]	
10/26/2022, 6:20:29.000 AM	Create	[redacted]	[redacted]	
10/26/2022, 6:20:31.000 AM	MoveToDeletedItems	[redacted]	[redacted]	
10/26/2022, 7:30:22.000 AM	MoveToDeletedItems	[redacted]	[redacted]	
10/26/2022, 7:30:47.000 AM	MoveToDeletedItems	[redacted]	[redacted]	
10/26/2022, 7:30:47.000 AM	SendAs	[redacted]	[redacted]	
10/26/2022, 7:32:44.000 AM	Update	[redacted]	[redacted]	
10/26/2022, 7:32:45.000 AM	Update	[redacted]	[redacted]	

Logs (continued)

- Unfortunately dealing with the logs is not always easy:
  - Schema not fully documented (even the basic fields)
  - Schema is fluid - new even types add new columns
  - Different logs do not provide consistent details of the event
    - Not all of them have geolocation, device/OS/browser information
  - Log records:
    - Never created for some operations
    - May arrive out of order
    - May be delayed (sometimes for hours)
    - Are occasionally lost
    - Expire after a period of time
- Microsoft is not treating log *contents* as a "contract" with the customer
  - SLAs exist for delivery, but available fields, data types and format may change without warning

Attack Tools

- As with on-prem environments, it's a good idea to perform periodic audits
  - External and internal Red Teams can verify that the defenses are solid
- A multitude (30+) of M365/AAD attack tools have been built by the community that can help imitate attacker behavior
- Majority of them specialize in password bruteforcing/sprays and recon
- Notable examples:
  - *AADInternals* (https://aadinternals.com/aadinternals/) - rich set of recon and attack behaviors from the expert in the field
  - *AzureHound* (https://github.com/BloodHoundAD/AzureHound) - a plug-in to BloodHound to collect information about AAD
  - *Vajra* (https://github.com/TROUBLE-1/Vajra) - GUI-based tool that does recon, password exploits, data exfil and consent grant attacks.

Defense Strategies

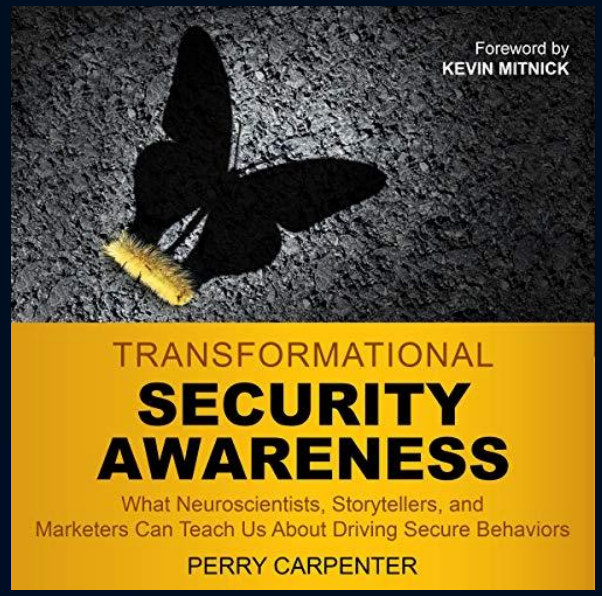
Preventing and Mitigating Attacks

- Continuously defending M365/AAD environment is different from defending an on-prem setup

- One needs to concentrate on 3 priorities:
  - Education
  - Configuration
  - Security Monitoring

Education

- Humans are the weak link in the security equation
  - And this is partially our fault as security technologists
- As we have seen above, some attack techniques exploit weaknesses in human abilities:
  - Users are notoriously bad at selecting secure passwords
  - Employees are easily tricked into clicking on links, opening attachments, and providing private information
- Preventing such attacks is a fine balance to strike
  - Overly permissive settings do not encourage secure behavior
  - Overly restrictive settings (mandated frequent changes of complex passwords, prohibition of links and attachments) may affect business efficiency
- Awareness is critical first step in attack prevention
- Train employees to recognize signs of phishing and BEC scams
- …but expect them to keep failing



Configuration

- Many of configuration recommendations are common sense
- M365 provides secure defaults for many settings, but that does not cover all scenarios

- Prevent account compromises
  - Introduce and enforce MFA
  - Reduce or remove legacy authentication vectors (e.g., IMAP)
  - Encourage password managers
  - Add password complexity requirements
  - Integrate with solutions that check for common weak passwords (e.g., check passwords against *Have I Been Pwned (HIBP)*, *rockyou*, and similar lists)
  - Consider using FIDO2 if available
  - Harden security of admin accounts

Configuration (continued)

- Enable sanitization of embedded links and attachments
- Turn on logging
- Audit user access rights, reduce to minimum required
- Configure Conditional Access
- Restrict guest access
- Restrict consent to apps
- …and more

- Review recommendations of Microsoft 365 Defender

Configuration - SSPM

- SaaS environment is constantly changing, with new users and groups created, permissions changed, applications installed
  - The challenge is to not only configure the environment securely, but to *maintain* secure posture
- M365/AAD has an estimated of *7500+ security settings per user*
- Expertise required to configure systems properly is not always available
- **Consider using a Cloud/SaaS Security Posture Management (CSPM/SSPM) solution**
  - SSPM provides an automated way of periodically verifying setting security

Security Monitoring

- Even with properly trained and alert workforce, and secured configuration, compromises are still possible
- Customer environment must be continuously monitored for malicious activity

"There are only two types of companies - those that know they've been compromised, and those that don't know."

Dmitri Alperovitch, CrowdStrike

- Companies that maintain a large security team could develop their own custom detection functionality
  - This requires specialized skills and continuous maintenance
- Sophistication and changing nature of attacks leads many companies to opt for *Cloud/SaaS Detection and Response (CDR/SDR)* tools
  - Logs can stay in Sentinel and Microsoft-provided detections can alert on malicious behavior
  - Logs can flow into an external SIEM and 3rd party detection functionality can alert on events

Security Monitoring (continued)

- Unfortunately, many tools are not perfect:
  - Alarm volume in a busy environment can be overwhelming
  - Blind spots exist
- Heuristic-based detection rules often cannot capture complex attacker behavior without too many "false positives"
  - For example, an employee connecting from a new country could be:
    - Employee on vacation or a business trip
    - Same employee using a VPN or a proxy
    - Attacker stealing the account
- Consider detection products that:
  - Analyze behavior based on **context** (history, environment trends, location, threat intelligence, etc.)
  - Are based on **Artificial Intelligence/Machine Learning**

Wrap-up

- M365 is a juicy target for attackers, and contains loads of valuable data that can be exploited
- Vast majority of attacks are fairly low-tech and stem from misconfigurations and social engineering; 0days in the infrastructure are addressed by Microsoft
- To secure your environment you need to:
  - Educate your workforce
  - Harden your security posture (MFA, hardened admin access, …)
  - Continuously monitor security configuration of your environment (CSPM tools), because your environment changes dynamically
  - Monitor your environment for malicious behavior, preferably with an intelligent CDR solution

Q&A

@0xd13a on Discord/Twitter

https://www.linkedin.com/in/beryozad

Slides can be found at https://github.com/0xd13a/presentations

Thank you!