WAVESTONE

Office 365
What are the current threats?
What are the actions to be taken quickly?

Cybersecurity & Privacy Insight Day | November 2020

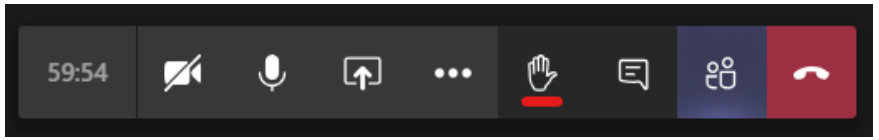
Thibault Joubert
Senior Consultant
Member of GT Clusif O365 & Security
MS500 - Microsoft 365 Security Administrator

A few precisions before starting the webinar

- 35 minutes presentation
- 10 minutes of Q/A

Guidelines for use:

- Keep the microphone off when the presenter is speaking
- Notify before speaking



This webinar is interactive and will be recorded.
Therefore, please note that any questions asked orally may be recorded in the replay of the webinar.

Microsoft OFFICE 365

1st COLLABORATIVE PLATFORM

50% of the worldwide Enterprise Messaging market

258 millions monthly active users in 2020 (**+21%**)

70% of **Fortune 500** companies have purchased Office 365

60% of EMEA companies use Office 365

80% of CAC40 companies use Office 365

Source: Microsoft, Wavestone

versus CYBERCRIME

A MOST WANTED TARGET

More than 50% of **the sensitive data** of the organizations

92 % of malware are delivered by emails

38% of phishing attack target SaaS services (1st before financial)

The most targeted brand since 2Q18

43% of all malicious attachments are Microsoft Office documents

Source: Verizon

Microsoft OFFICE 365

1st COLLABORATIVE PLATFORM

50% of the worldwide enterprise Messaging market

258 millions monthly active users in 2020 (**+21%**)

70% of **Fortune 500** companies have purchased Office 365

80% of companies use Office 365

60% of CAC40 companies use Office 365

Source: Microsoft, Wavestone

versus CYBERCRIME

A MOST WANTED TARGET

More than 50% of **the sensitive data** of the organizations

92 % of malware are delivered by emails

38% of phishing attack target SaaS services (1st before financial)

since 2Q18

43% of all malicious attachments are Microsoft Office documents

Source: Verizon

With 3 main motivations *in the end…*

Financial gains

Data theft

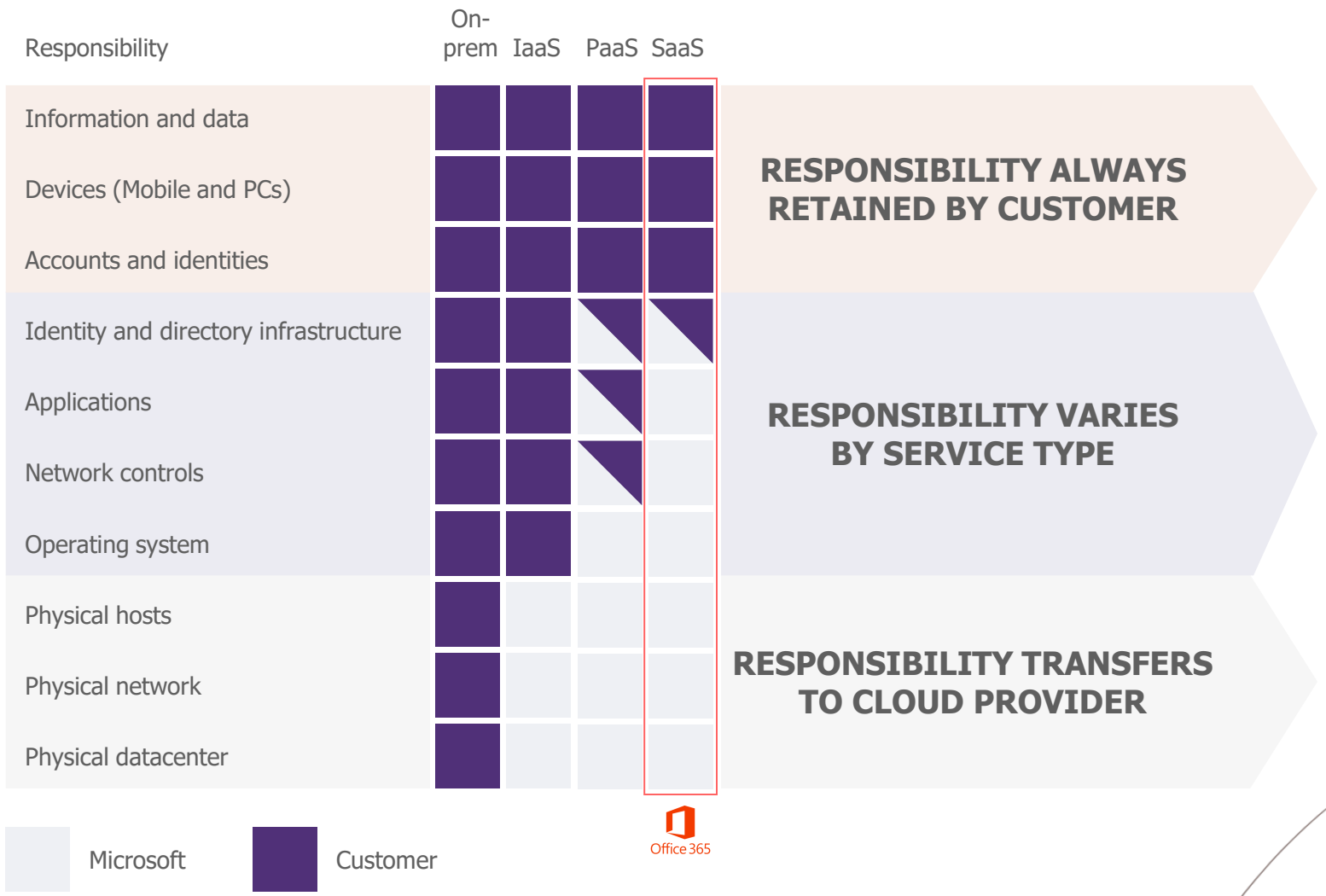
Credential harvesting and rebounce

What are the **main** **CYBER TOPICS** *with* **Office 365** **?**

AS-A-SERVICE SHARED RESPONSIBILITY MODEL

Good news:
Microsoft provides a secure platform and services… You "only" need to focus to users/data/devices and to read "Service Trust Portal" to understand security around Microsoft Infrastructure

Bad news:
Misconfiguration, Phishing, Zero Day Malware, Information protection, Compliance, Account takeover…



What are the **main CYBER TOPICS** *with* **Office 365 ?**

AS-A-SERVICE SHARED RESPONSIBILITY MODEL

Good news:
Microsoft provides a secure platform and services… You "only" need to focus to users/data/devices and to read "Service Trust Portal" to understand security around Microsoft Infrastructure

Bad news:
Misconfiguration, Phishing, Zero Day Malware, Information protection, Compliance, Account takeover…

IDENTITY IS THE NEW PERIMETER

"Defenders think in lists. Attacks think in graphs. As long at it is true, attackers wins."

Traditional VPN and certificated based authentication do no longer guarantee the identity and the compliance of a connection

Old world vs **new world**

Users are the employees
→ **Internal, partners, clients…**

Devices are managed by the company
→ **BYOD ("Bring Your Own Device")**

Applications are used on our network
→ **Everything is going in the Cloud**

Internal network and firewall
→ **No more perimeter**

Local footprints
→ **A lot, lot more signals!**

What are the **main CYBER TOPICS** *with* **Office 365 ?**

AS-A-SERVICE SHARED RESPONSIBILITY MODEL

Good news:
Microsoft provides a secure platform and services… You "only" need to focus to users/data/devices and to read "Service Trust Portal" to understand security around Microsoft Infrastructure

Bad news:
Misconfiguration, Phishing, Zero Day Malware, Information protection, Compliance, Account takeover…

IDENTITY IS THE NEW PERIMETER

"Defenders think in lists. Attacks think in graphs. As long at it is true, attackers wins."

Traditional VPN and certificated based authentication do no longer guarantee the identity and the compliance of a connection

SECURITY TEAMS RARELY INVOLVED

The migration is over…

But security should not be forgotten and left aside!

Think cybersecurity by design

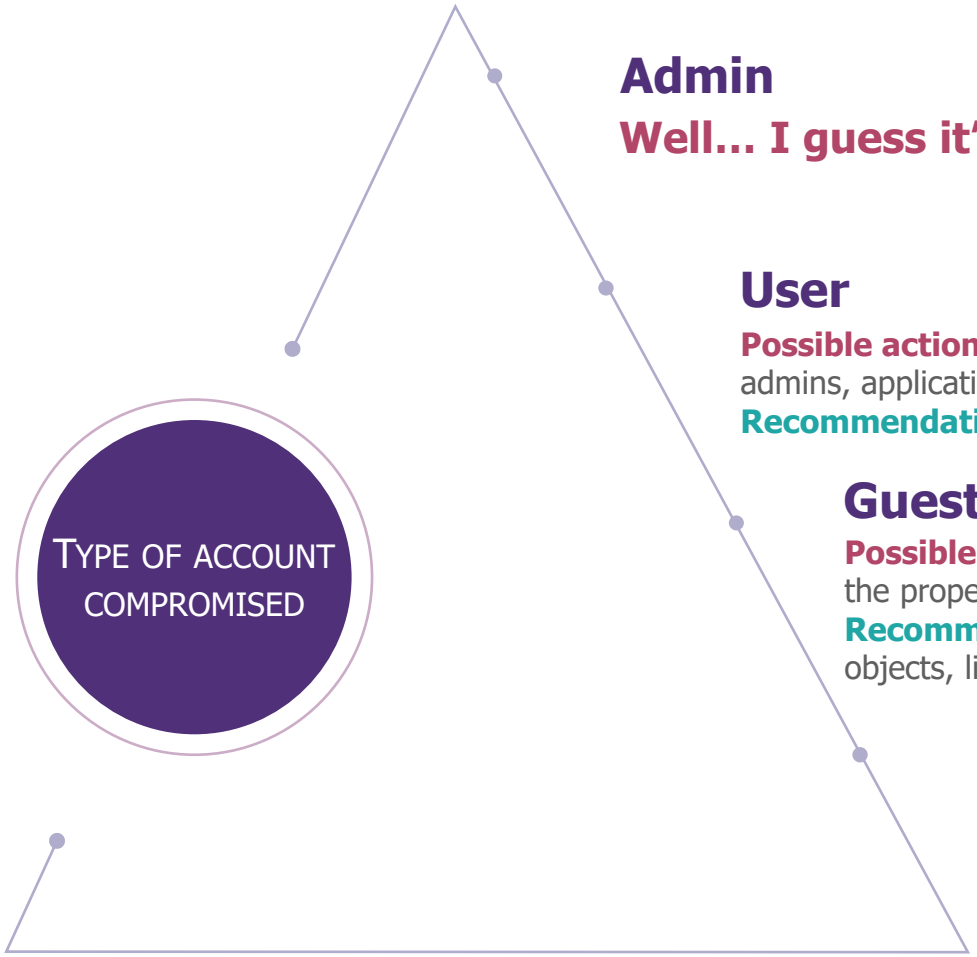
To anticipate, watch your company *with* **CYBERCRIMINAL** *eyes*

RECONNAISSANCE | INITIAL ACCESS | LATERAL MOVEMENTS | ACTION ON OBJECTIVES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	CMSTP	Accessibility Features	Accessibility Features	Bypass User Account Control	Credential Dumping	Account Discovery	Logon Scripts	Data Staged	**Remote Access Tools**	Data Compressed
Spearphishing Link	Command-Line Interface	Logon Scripts	Bypass User Account Control	CMSTP		Network Service Scanning	Remote Desktop Protocol	Automated Collection	Remote File Copy	Data Encrypted
Valid Accounts	Dynamic Data Exchange	New Service	Exploitation for Privilege Escalation	File Deletion		Permission Groups Discovery	Remote File Copy		Standard Application Layer Protocol	
Exploit Public-Facing Application	Exploitation for Client Execution	Redundant Access	New Service	Indicator Removal from Tools		Process Discovery	Windows Admin Shares		Standard Cryptographic Protocol	
	PowerShell	Registry Run Keys / Startup Folder	Process Injection	Masquerading		**Remote System Discovery**			Web Service	
	Regsvr32	Scheduled Task	Scheduled Task	Obfuscated Files or Information		Security Software Discovery				
	Scheduled Task	Valid Accounts	Valid Accounts	Process Injection						
	Scripting	Web Shell	Web Shell	Redundant Access						
	Service Execution			**Regsvr32**						
	Signed Binary Proxy Execution			**Scripting**						
	User Execution			Signed Binary Proxy Execution						
	Windows Management Instrumentation			XSL Script Processing						
	XSL Script Processing			Valid Accounts						
				Web Service						

MITRE | ATT&CK™

RECONNAISSANCE *phase*
What information can be exploited?



Admin
Well… I guess it's too late ;-)

User
Possible actions: dump Azure Active Directory: usernames (incl. sync, last connection…), groups, admins, applications, etc..
Recommendations: limit access to Azure Portal and programmatic access (PowerShell, Graph API)

Guest (Azure B2B identity or Office 365 sharing)
Possible actions: get some Azure AD settings, list most applications, internal users, groups by reading the properties of the groups to which it has access.
Recommendations: restrict guest user access to properties and memberships of their own directory objects, limit access to Graph API

External (no access to the tenant)
Possible actions: access public information about identity management (federation or Cloud), mail architecture (primary gateway, SPF, DKIM, DMARC, etc.). Test the existence of users silently (e.g. test One Drive site, Seamless SSO, AutoDiscover) or not (ActiveSync, login page)
Recommendations: nothing to do but show a good hygiene

INITIAL ACCESS *phase*

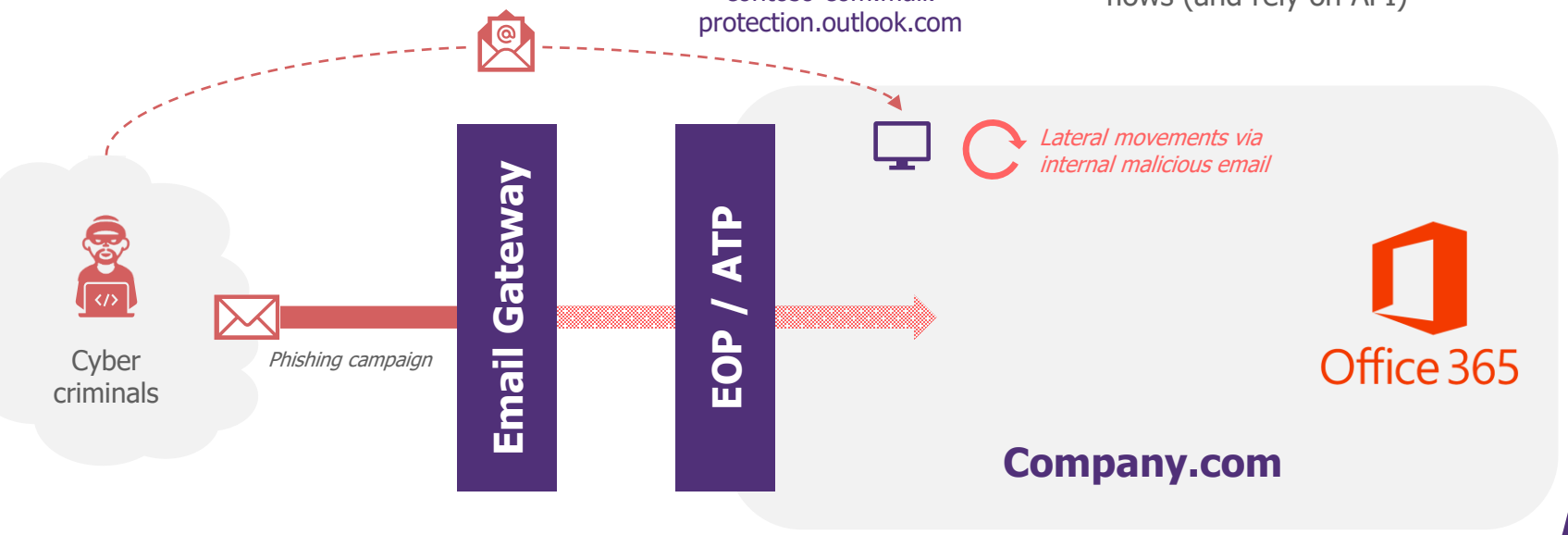
How the attack is delivered?

Risk: by-pass of mx records

Recommendation: lock down EOP to prevent email to enter directly

Risk: Internal threat, once compromised

Recommendation: Cover all flows (and rely on API)



Risk: Target of Email Gateway / EOP limitations: obfuscation, link in attachment, captcha

Risk: Loss of signal between primary gateway and EOP

Recommendation: assess if EOP to be implemented as the primary gateway or enable Enhanced Filtering

~99% of email attacks require a **manual action** (Microsoft, Verizon)

WHY ARE MY USERS TAKING THE BAIT?

Used to look & feel

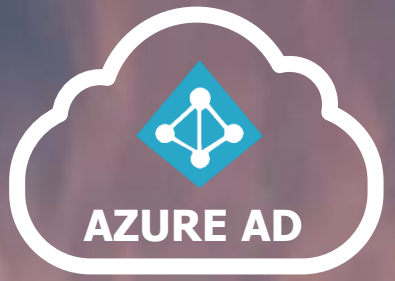
Access to online documents

Action required

User impersonation

Initial foothold on Office 365

are mainly **IDENTITY BASED…**



CREDENTIAL	TOKEN	OAUTH
Collection of the user's credentials (login / password) to authenticate in his place	**Interception of access / refresh tokens** and reuse by the attacker	**Delegation of consent** to a malicious application on user's data, emails and settings

… and can be mainly covered with a good hygiene and a relevant Zero Trust strategy

CREDENTIAL HARVESTING

Old-fashioned but still widely used

CREDENTIAL HARVESTING

Old-fashioned but still widely used

(Spear) Phishing

Mislead the user to collect his credentials

- 30% of phishing attacks target Microsoft accounts (Verizon, DBIR 2020)
- Sending the user to a forged login page
- Still 10-30% of users falls into the trap
- Only 7% of Microsoft accounts are covered by MFA
- All services (e.g. Azure Portal) are not always MFA protected

➔ **Enforcing MFA good, registering it better!**

Password spray

Test the most frequently used passwords on identified accounts

- Ex: Early 2020, 30 000 were tested in 2 days (all ingredients are available on the internet)
- 99% of password spray based on legacy protocols, such IMAP, POP, etc. (Microsoft)
- Legacy protocols do not support MFA and will be depreciated for the second half of the second half of 2021

➔ **Do not wait 2021 to cut legacy protocols (with Conditional Access AND admin center)**

TOKENS INTERCEPTION

MFA is not a silver bullet

TOKENS INTERCEPTION

MFA is not a silver bullet

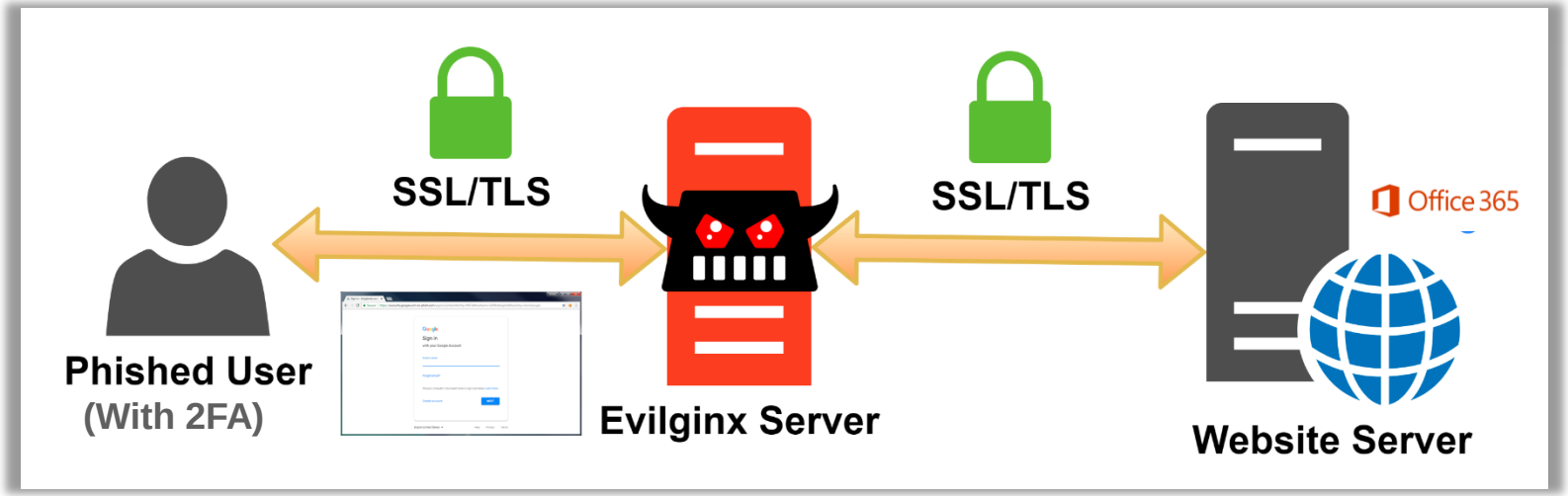
Refresh token with MITM attack (2018)

Combination of phishing with real time verification and reverse proxy (e.g. Evilginx2)

- Relay between the user and the applications
- Server collect the credentials and the authentication token after a simple / multi factor authentication

➔ **From MFA to Conditional Access**

An example of MITM attack with Evilginx2 for O365 (2018)



> Instead of serving templates of sign in pages lookalikes, Evilginx becomes a relay between the real website and the phished user. Phished user interacts with the real website, while Evilginx captures all the data being transmitted between the two parties.

https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

Effective counter-measures within Office 365

- U2F
- Conditional Access with IP
- Conditional Access with joined device
- Conditional Access with compliant device
- IDP accessible only through VPN
- IDP with certificate based authentication

TOKENS INTERCEPTION

MFA is not a silver bullet

Refresh token with MITM attack (2018)

Combination of phishing with real time verification and reverse proxy (e.g. Evilginx2)

- Relay between the user and the applications
- Server collect the credentials and the authentication token after a simple / multi factor authentication

➔ **From MFA to Conditional Access**

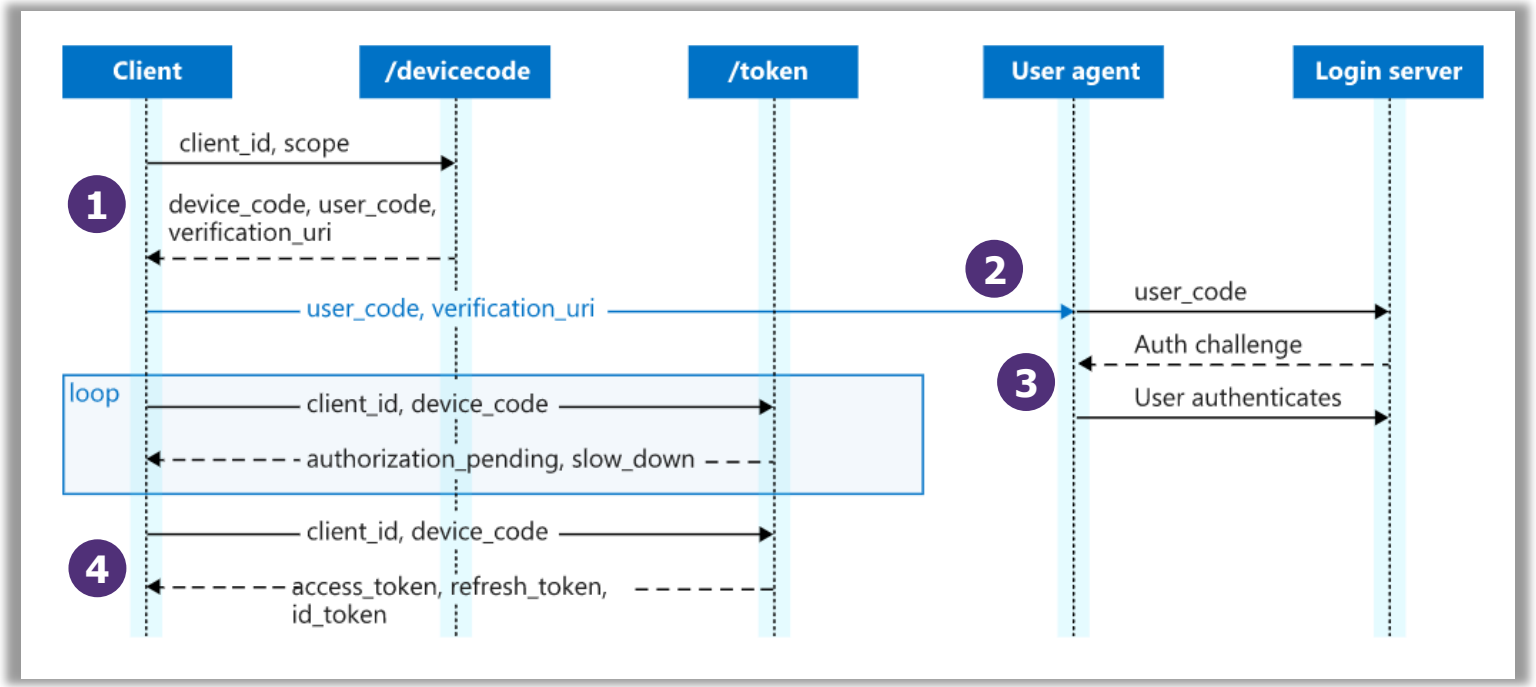
Refresh token with device code attack (2020)

Simulate an input-constrained device to request an authentication on a trusted environment

- Rely on OAuth device code protocol (Very simple to implement)
- By design, Azure AD sees only attacker context
- Most of company are today vulnerable (e.g. against third-party conditional access: IP or certificate-based authentication)

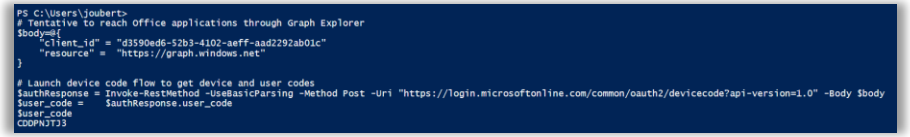
➔ **Evaluation of context must be performed for the authorization not the authentication**

An example of device code attack (2020)

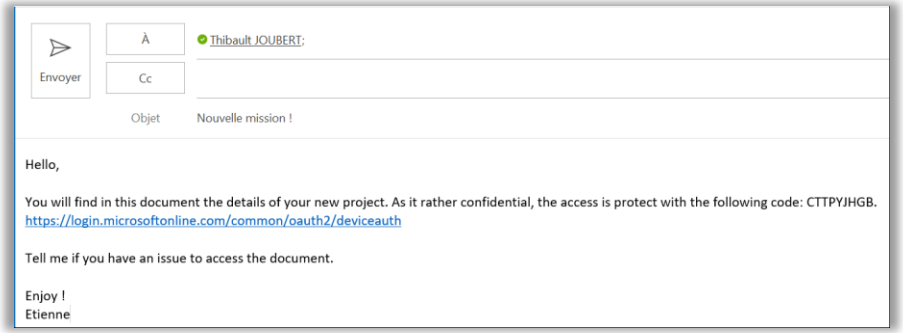


1. An attacker **connects to /devicecode** endpoint and sends client_id and resource to get user_code and verification_uri
2. Send to the victim **the verification_uri** (https://login.microsoftonline.com/common/oauth2/deviceauth) **and user_code**
3. Victim **clicks the link, provides the code and completes the sign in** (according the authentication policy in place)
4. The attacker **receives access_token and refresh_token** and can now mimic the victim

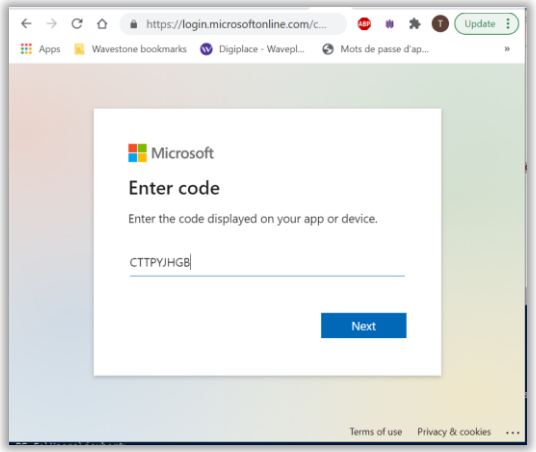
An example of device code attack (2020)



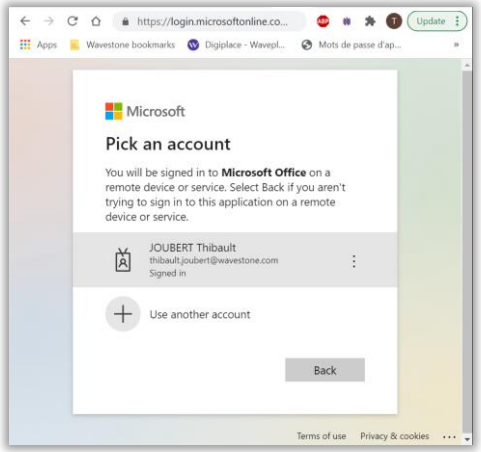
The attacker launches device code flow



Share the bait: sensitive document



The user enter the provided code in the 100% Microsoft url



After the usual authentication (in a trusted context), the attacker gets an access token

The authentication of the user is performed in a trusted environment

The only clue is the fact the request to access O365 comes from the attacker's context

Effective counter-measures within Office 365

- AAD / CASB Conditional Access with IP address
- AAD / CASB Conditional Access with device joined
- AAD / CASB Conditional Access with compliant devices
- CASB with certificated verification

Refresh token with MITM attack (2018)

Combination of phishing with real time verification and reverse proxy (e.g. Evilginx2)

- Relay between the user and the applications
- Server collect the credentials and the authentication token after a simple / multi factor authentication

➔ **From MFA to Conditional Access**

Refresh token with device code attack (2020)

Simulate an input-constrained device to request an authentication on a trusted environment

- Rely on OAuth device code protocol (Very simple to implement)
- By design, Azure AD sees only attacker context
- Most of company are today vulnerable (e.g. against third-party conditional access: IP or certificate-based authentication)

➔ **Evaluation of context must be performed for the authorization not the authentication**

TOKENS INTERCEPTION

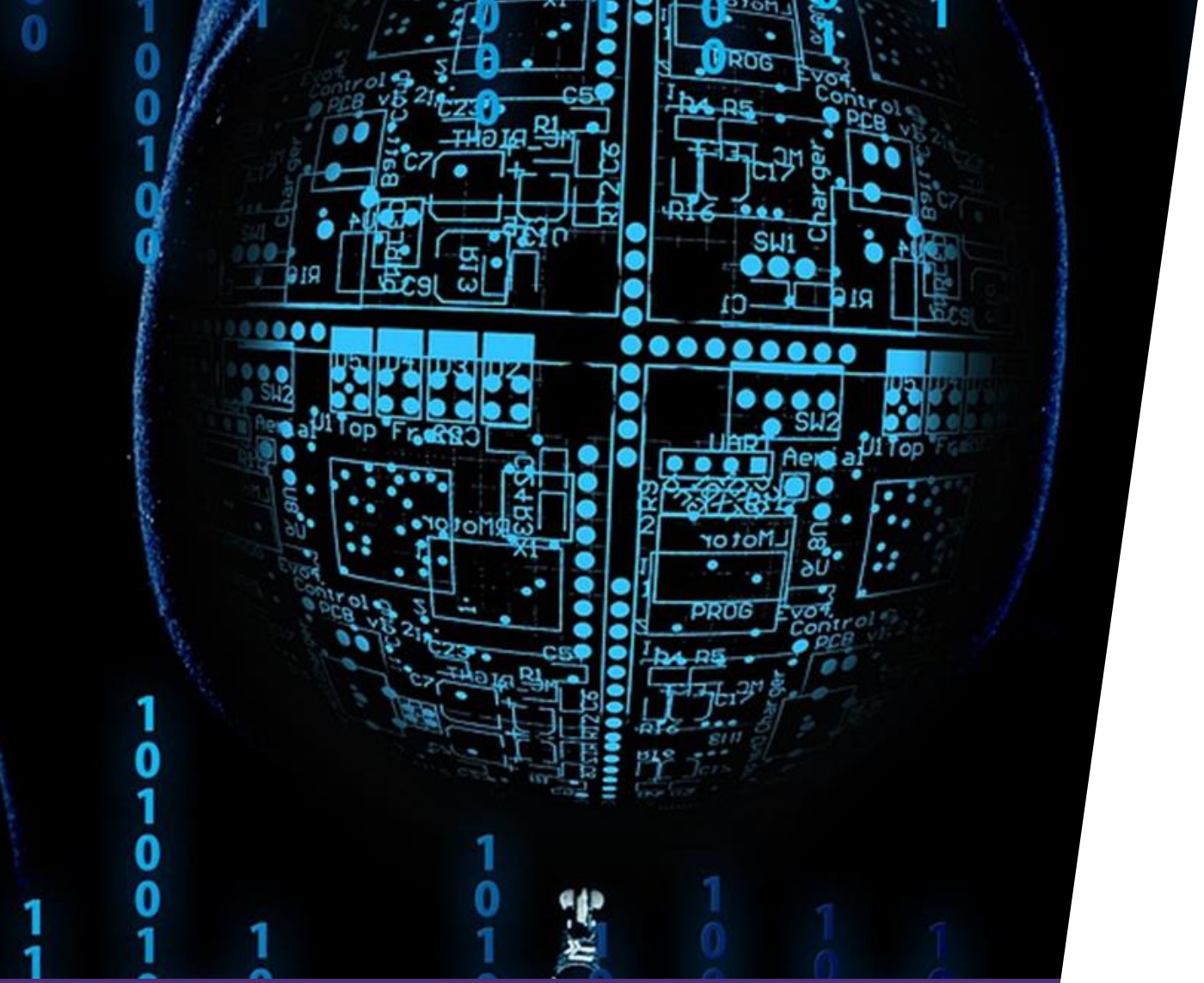
MFA is not a silver bullet

CONDITIONNAL ACCESS

Evaluation of context must be performed for the authorization not the authentication

OAUTH CONSENT

A wolf in sheep's clothing



OAUTH CONSENT

A wolf in sheep's clothing

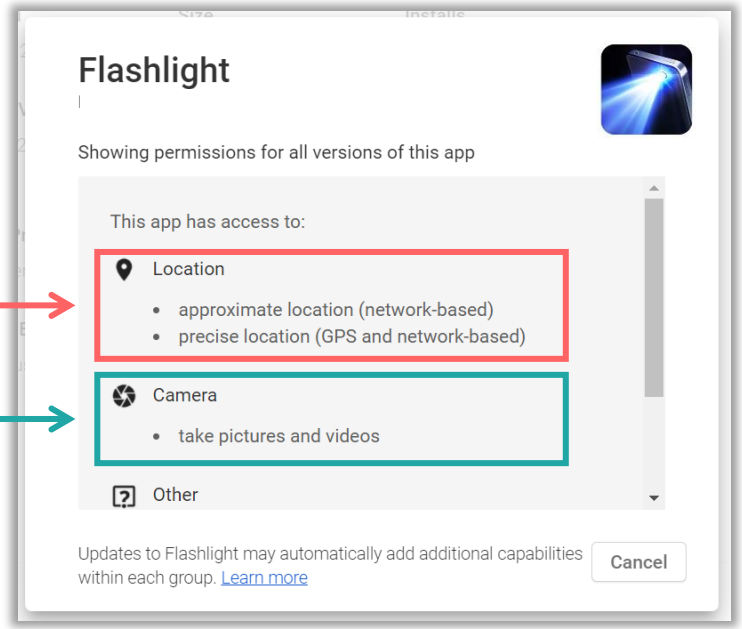
Azure AD Applications

Mislead users to grant permissions

- OAuth framework allow authorized third-party apps to perform action on the behalf of a user
- By default, a user can give consent for "non sensitive permissions". But sensitive is relative!
- Ex: Synchronization OneDrive to Google Drive
- Ex: Dump of Azure Active Directory

➔ **Prevent users to give their consent and define an application management process**

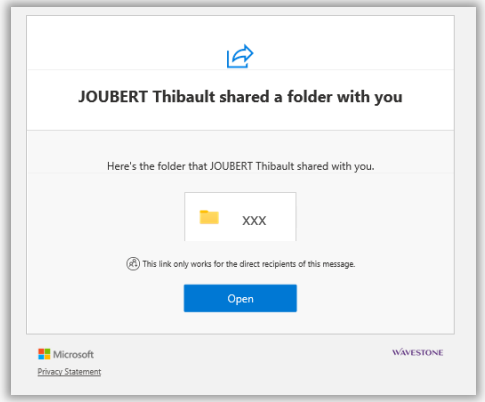
Remember this?



Legitimate permissions?

Legitimate permissions

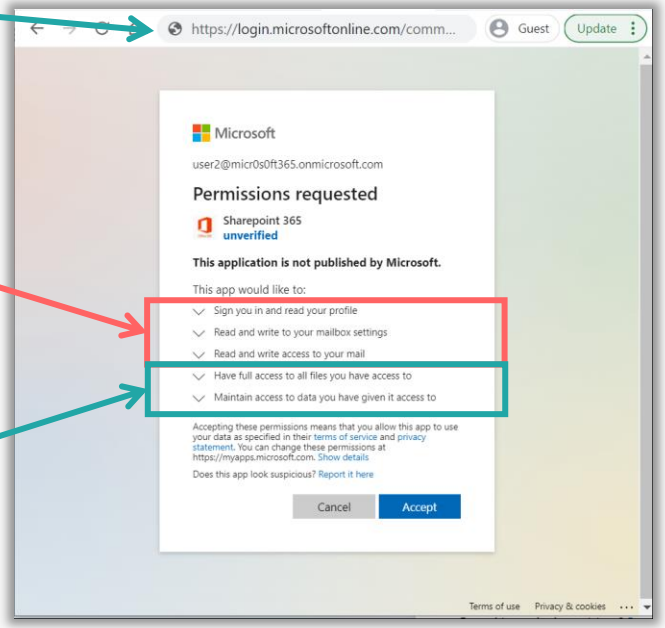
IT'S THE SAME THING FOR O365!

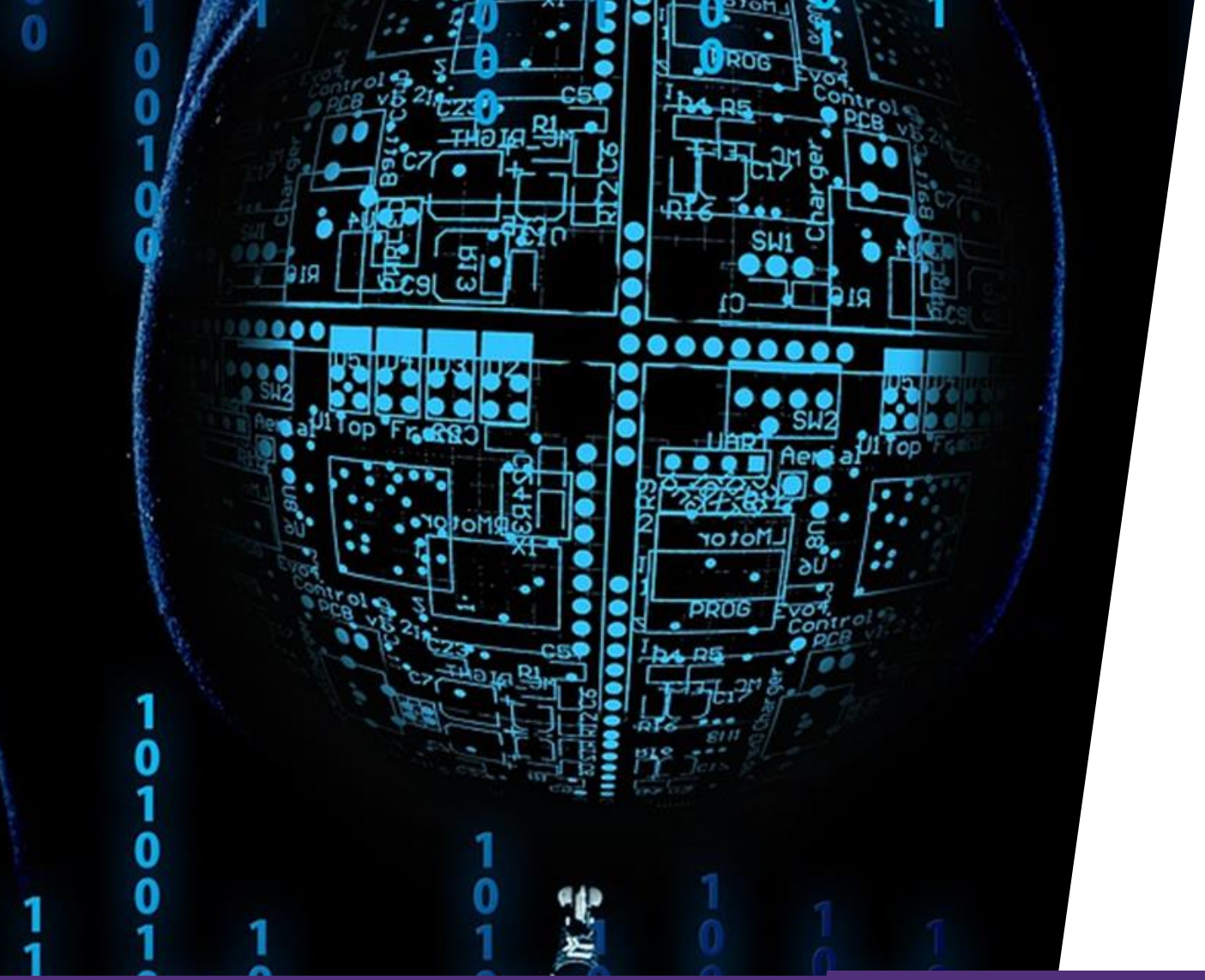


Url 100% Microsoft

Legitimate permissions?

Legitimate permissions





Azure AD Applications

Mislead users to grant permissions

- OAuth framework allow authorized third-party apps to perform action on the behalf of a user
- By default, a user can give consent for "non sensitive permissions". But sensitive is relative!
- Ex: Synchronization OneDrive to Google Drive
- Ex: Dump of Azure Active Directory

➔ **Prevent users to give their consent and define an application management process**

OAUTH CONSENT

A wolf in sheep's clothing

MANAGE THIRD-PARTY APPS

And include SharePoint, Office, Teams, Power Automate, Power BI add-ins and connectors

How to keep a foothold within Office 365?

Create a guest account

| *Less strict Conditional Access & No lifecycle*

Registration of a new application with the associated secret

| *User Impersonation*

| *Privilege escalation (if the Application Admin role is compromised)*

Consent permissions to Azure AD third applications

| *User Impersonation with the use of OAuth permission*

Creation of email transfer rule within Exchange Online

| *Full of partial transfer of incoming emails to an external mailbox*
Note that Microsoft is to switch Automatic forwarding to "Off" by default

Creation of a Power Automate (ex-Microsoft Flow)

| *The use of Power Automate cannot be blocked (but connector can be prevented to access business data)*

| *By-pass of email transfer interdiction rule, Synchronization of documents, etc.*

Attackers mainly rely on lack of governance and basic hardening

**Most of the ~10 Office 365 audits carried out this year did not comply with these controls*

LATERAL MOVEMENTS *phase and …*
Searching a target

More phishing … more persistence …

More phishing … more persistence …

More phishing … more persistence …

Until finding interesting accounts (VIP, Global accounts, "shadow admins" as Application Admin or Privileged Administrator Account)

… **ACTION ON OBJECTIVES** *phase*
Bingo!

Business Email Compromise

Data theft (e.g. automated with workflow or API)

Data destruction (e.g. with retention policy)

Corporate spying

eDiscovery
Graph API
Retention label

What **MUST** *you have in* **your Office 365 security roadmap?**

01

Back to basics

Now:

/ Review the opening and the hardening of the services
/ Meet your workplace counterpart and work together
/ Raise awareness

Tomorrow:

/ Keep Evergreen

02

Authentication

Now:

/ Adopt MFA, disable legacy authentication, enforce smart lock out
/ Reinforce password settings

Tomorrow:

/ Build your modern workplace with UEM
/ Implement a true conditional access
/ Go passwordless
/ Sync the hashes into the Cloud for resilience purposes

03

Emails

Now:

/ Review EOP settings and Exchange Transport Rule to filter emails
/ Implement anti-spoofing

Tomorrow:

/ Migrate your gateway in the Cloud and cover all flows and emails at rest

04

Privileged access management

Now:

/ Review your privileged admins

Tomorrow:

/ Leverage Microsoft advanced capabilities with cloud accounts (, Azure PIM, Azure AD Id Protection, etc.)

05

Detection & Reaction

Now:

/ Keep your logs
/ Know of to react in case of comprise

Tomorrow:

/ Think your supervision to cover the main threat and common attacks (MITRE ATT&CK)
/ Leverage Security Graph API and advances tools machine learning to support your SOC teams

The Positive Way

WAVESTONE

THANK YOU