WAVESTONE

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

Clusis 5 à 7 | October 2021

Thibault Joubert @Wavestone Lyon (FR)
Manager Cybersecurity & Digital Trust
Member of GT Clusif O365 & Security
MS500 - Microsoft 365 Security Administrator

Rémi Pactat @Wavestone Geneva (CH)
Manager Cybersecurity & Digital Trust
Wavestone CH is Sponsor of Clusis
Program Mgt, Risks analysis, audits

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** *versus* **CYBERCRIME**

1st COLLABORATIVE PLATFORM

A MOST WANTED TARGET

With **3 main motivations** *in the end…*

50% of the worldw[illegible]terprise Messaging market

258 millions monthly active use[illegible]2020 (**+21%**)

70% of **Fortune 5**[illegible]mpanies have purchased Office 365

80% o[illegible] companies [illegible]e Office 365

60% of CAC40 companies use Office 365

Source: Microsoft, Wavestone

Financial gains

Data theft

Credential harvesting

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)

most targeted brand since 2Q18

43% of all malicious attachments are Microsoft Office documents

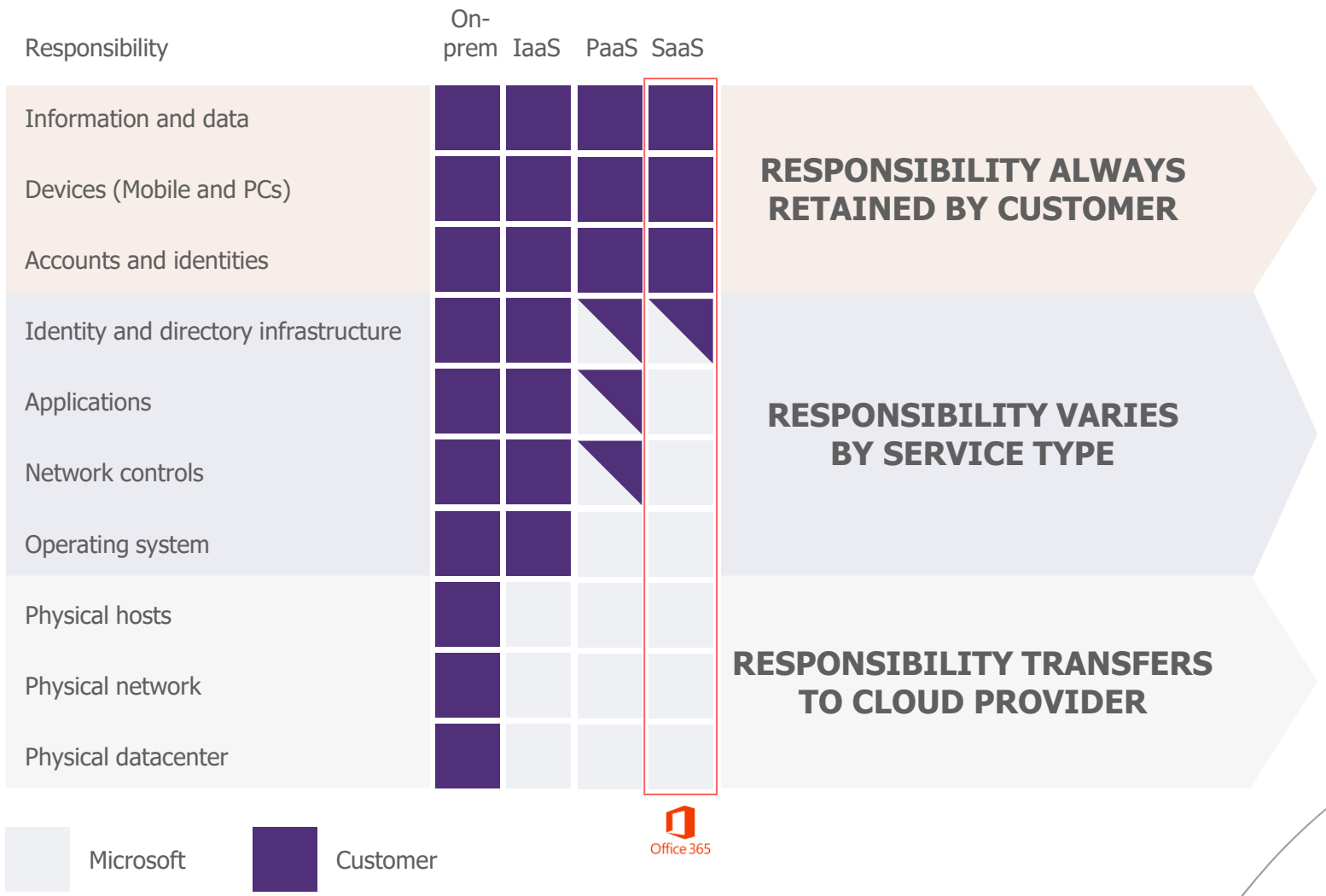
Source: Verizon

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*

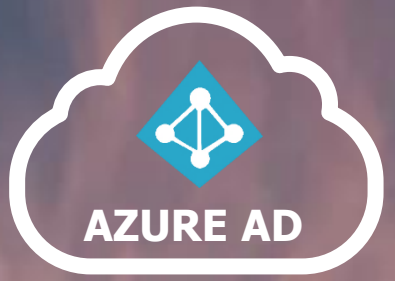
RECONNAISSANCE | INITIAL ACCESS | LATERAL MOVEMENTS | ACTION ON OBJECTIVES

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™

Initial foothold on Office 365

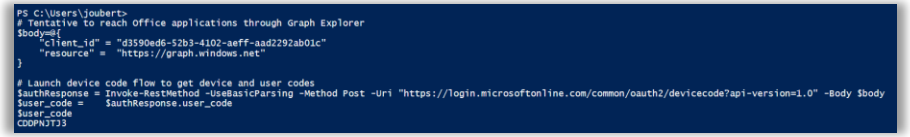
are mainly **IDENTITY BASED…**



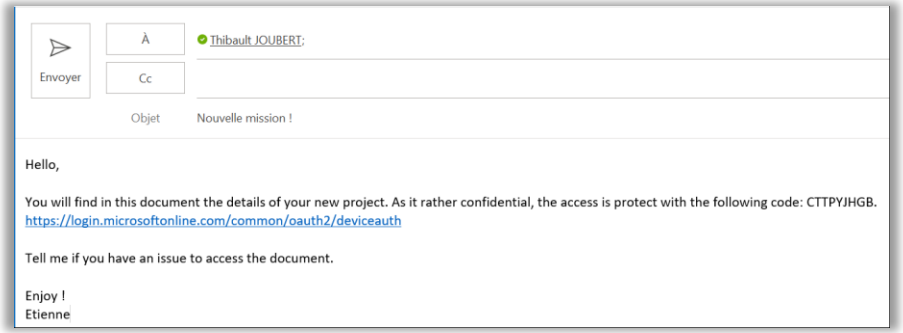
CREDENTIAL	TOKEN	OAUTH
Collection of the user's credentials (login / password) to authenticate in his place	**Interception of access / refresh tokens** and reuse by the attacker	**Delegation of consent** to a malicious application on user's data, emails and settings

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

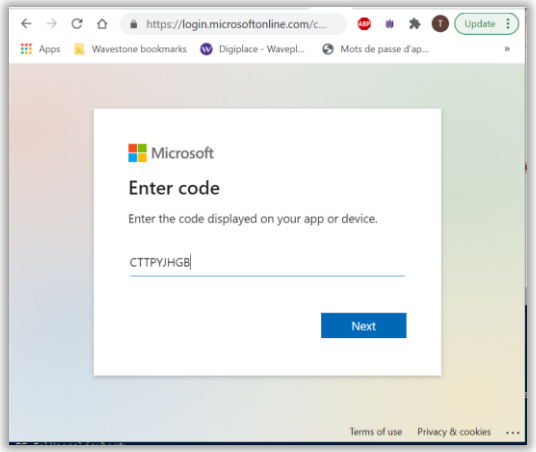
An example of device code attack (2020)



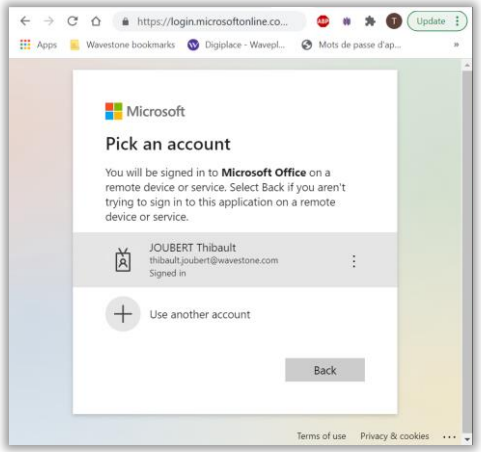
The attacker launches device code flow



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

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*

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

Thibault JOUBERT
Senior Consultant

M +33 (7) 63 97 33 59
thibault.joubert@wavestone.com

Rémi PACTAT
Manager

M +41 (0)79 395 13 42
remi.pactat@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILANO *

BRUSSELS

GENEVA

CASABLANCA

ISTANBUL *

EDINBURGH

LYON

MARSEILLE

NANTES

* Partnerships

WAVESTONE