

Fishnet Cases: How Microsoft Azure Helps with a Phishing Attack

Olga Karelova

Head of Security Analysis, «M 13» Ltd.

Who am I



- CTF team's "rm -rf" captain (rm -rf is VolgaCTF's winner in 2012 & 2013)
- M*CTF competition technical director in 2014–2016
- Associate Professor of the Department of Cryptology and Cyber Security, MEPhl
- Head of Security Analysis of Information Systems, «M 13» Ltd



Phishing problems



- Many companies use Microsoft as a mail service
- Some phishing letters detected as spam
- Some phishing letters detected as junk
- We need a lot of time to test new phishing methods
- We need a lot of time to test new payloads

Hypothesis



Maybe we can use some Microsoft protection products for our phishing company?



Microsoft Enterprise Mobility + Security (EMS)



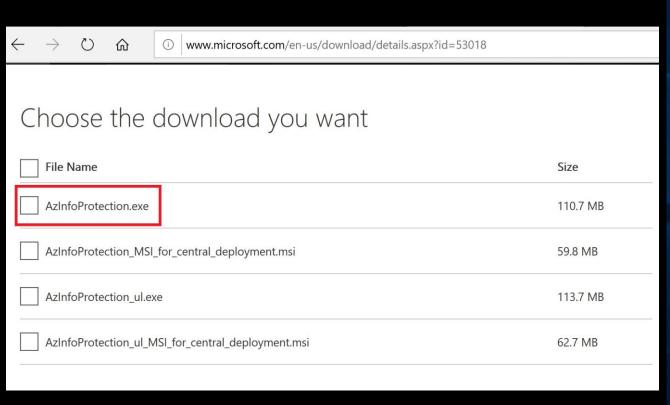
- Azure Active Directory
- Microsoft Intune
- Azure Information Protection
- Microsoft Cloud App Security
- Microsoft Advanced Threat Analytics
- Azure Advanced Threat Protection

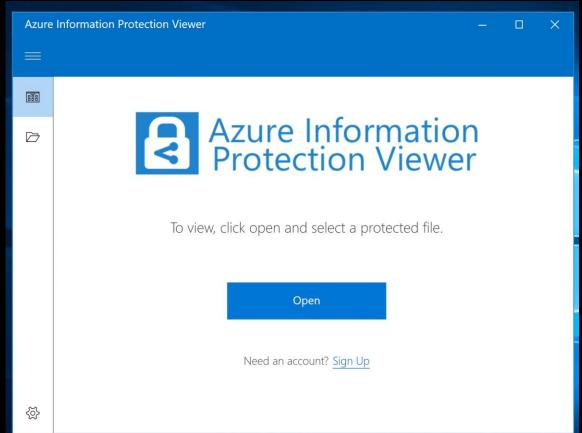
Azure Information Protection

Some information about AIP



AIP – solution which helps to classify your information





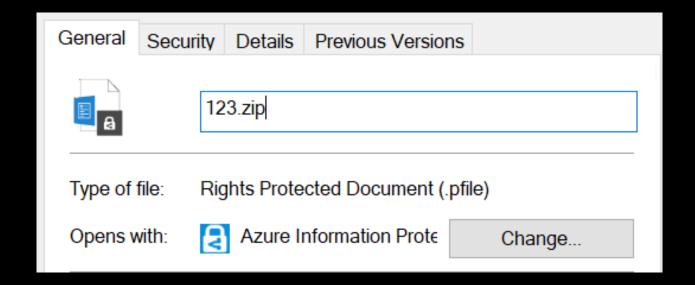
Some information about AIP

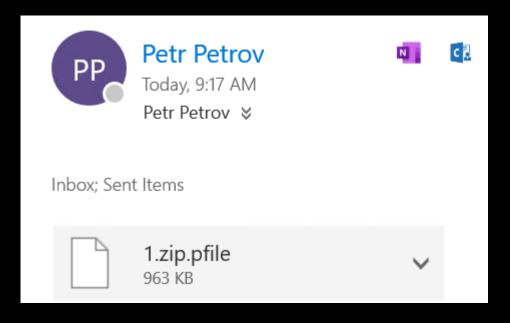


Classify and protect - Azure	Information Protection (Protection-only mo	ode)		-	· 🗆 ×		
1.txt	Classify and protect - Azure Information I	Protection (P	Protection-only mode	e)	×		
No protection	≙ 1.txt		Classify and prote	ct - Azure Information F	rotection (Protection-only mode)		– 🗆 X
Company pre-defined prot	O No protection		△ 1.txt		View Permis:	ion 🏻 Track and Revoke	? Help and Feedback
Select Template Not prot	Company pre-defined protection		O No protection				
O Custom permissions	Select Template Confidential \ All Emp	loyees	O Company pre-c	lefined protection			
Select permissions	Custom permiss Confidential \ All Empl	loyees	Select Template	Confidential \ All Empl	oyees		~
Select users, groups, or orga	Select permissions Highly Confidential \ A	All Employed	Custom permis	sions			
	Select users, groups, or organizations	Example: .	Select permission	S	Select Permission		~
			Select users, grou	ps, or organizations	Viewer - View Only		
					Reviewer - View, Edit		
					Co-Author - View, Edit, Copy, Print		
					Co-Owner - All Permissions		
Expire access	Final and a second				Only for me		
	Expire access	Never (Cli					
			Expire access		Never (Click to set an expiration date)		1000
						Apply	Close

Some information about AIP







What we need for research?



Microsoft Business Account (Microsoft 365 Business, 1250 rub/month per user)

• 2 companies (attacker and victim)

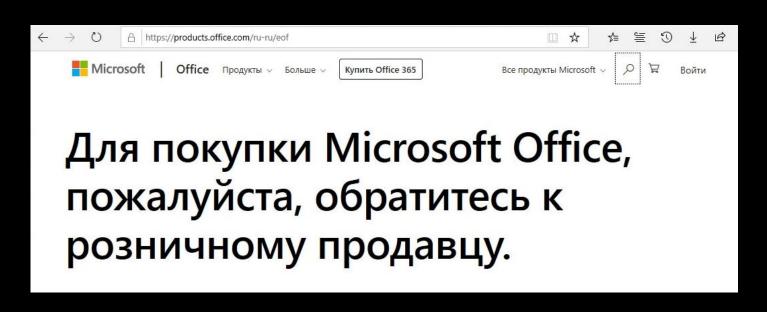
Some malicious document for phishing letters

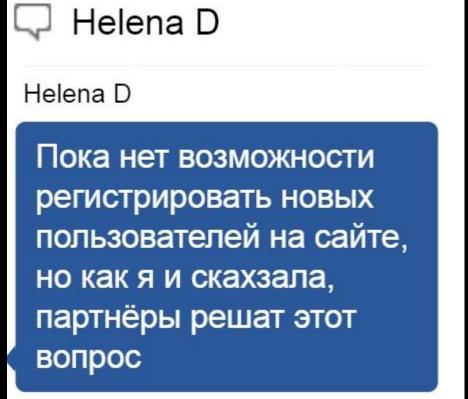
Creating Microsoft account

Ooooops! Some problems...



You can't create Microsoft Business Account from Russia







Helena D

Helena D

Чем занимается ваша компания?

Helena D

Сколько сотрудников в вашей компании?

Helena D

Сколько из них является пользователями?

Helena D

Являетесь ли вы уже пользователями продуктами Microsoft или конкурентов?



Helena D

Helena D

Какое у вас текущее решение? (сервер? ОП Windows? Office?)

Helena D

Есть что-то, что вас не устраивает? "Болевые точки"?

Helena D

Хотели бы вы что-то изменить или добавить?

Helena D

Новое решение? Почему именно это?



Sanctions detected



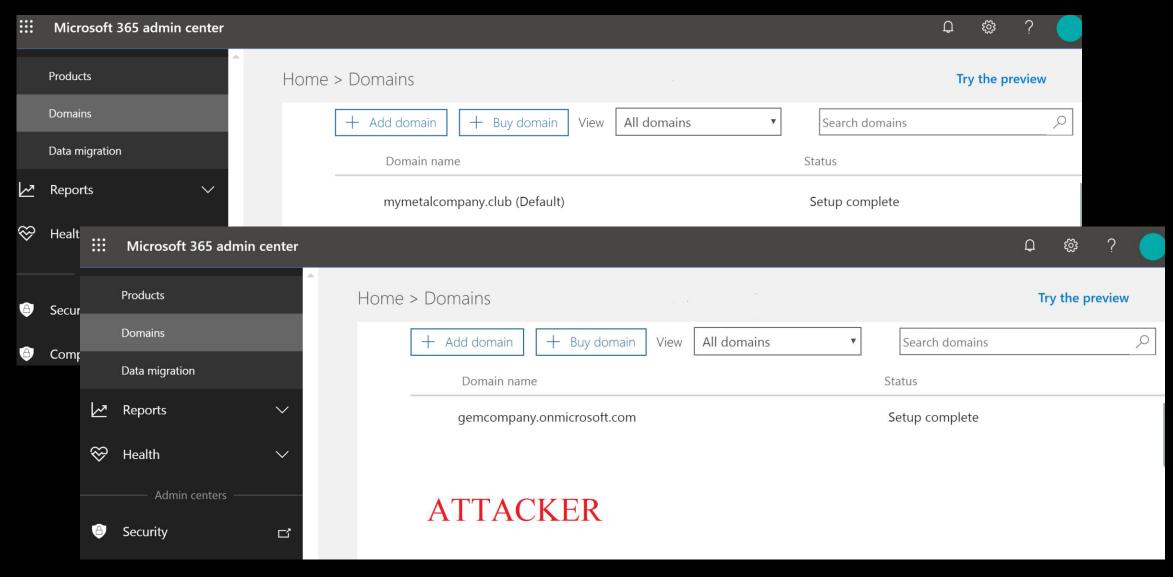
 You can't create Microsoft Business Account from Russia because sanctions.

 Russian IPs, Russian phone, Russian post code – bad for Microsoft

But Microsoft partners can create accounts for customers

Create attacker and victim accounts





Create attacker and victim accounts

VICTIM 1



VICTIM 2

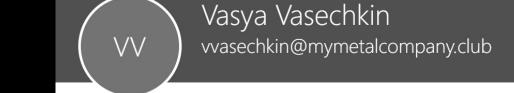


User was added

Display Petr Petrov

name

Username ppetrov@mymetalcompany.club



User was added

Display Vasya Vasechkin

name

Username vvasechkin@mymetalcompany.club



User was added

Display Evil User

ATTACKER

name

Username evil@gemcompany.onmicrosoft.com

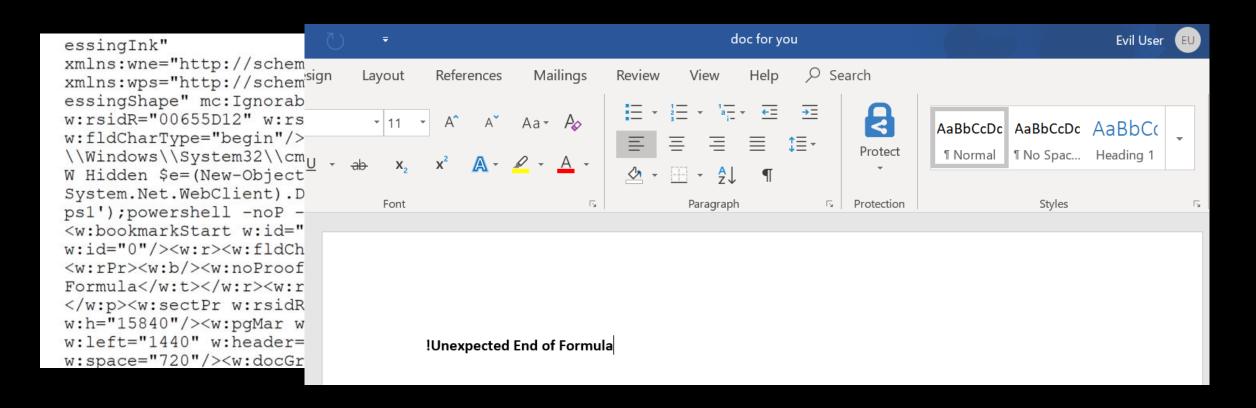
Testing

Malicious Doc



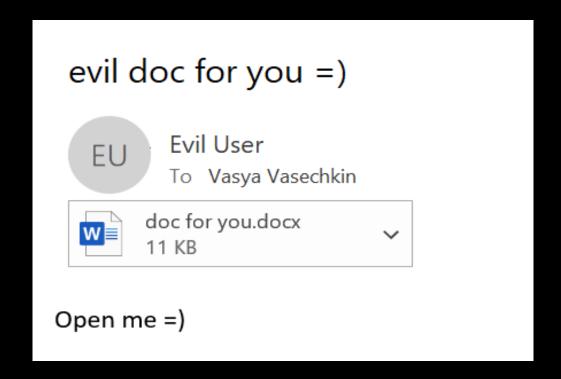
Exploit:O97M/DDEDownloader.B

(Quarantined)



Sent malicious document to user





But we can't find this mail in Vasechkin's Inbox



Microsoft blocked it!

Protect Malicious Doc



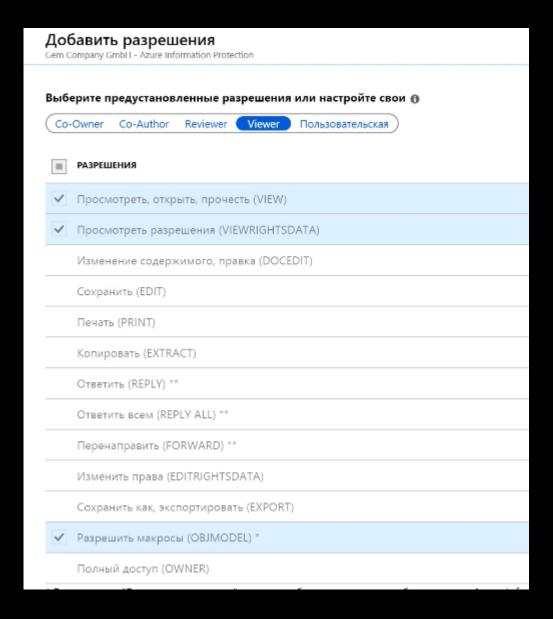
assify and protect - Azure Information Protection (Protection-only mode) — 🔲 🔀						
doc for you.docx	View Permission 🗂 Track and Revoke	? Help and Feedback				
O No protection						
Company pre-defined protection						
Select Template Not protected (click to	select template)	~				
Custom permissions						
Select permissions	Viewer - View Only	~				
Select users, groups, or organizations	vvasechkin@mymetalcompany.club	ŢĮ.				
Expire access	Never (Click to set an expiration date)					
	Apply	Close				

Vasechkin can open malicious doc

Others – can't open this doc

Viewer is a great permissions for user



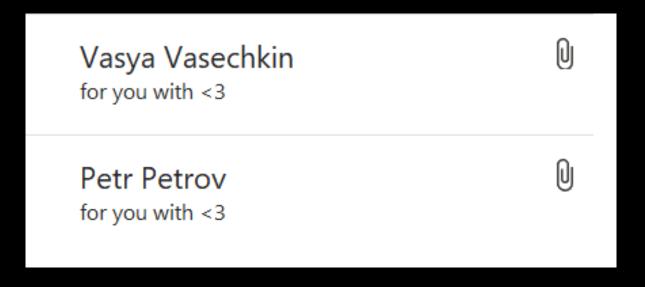


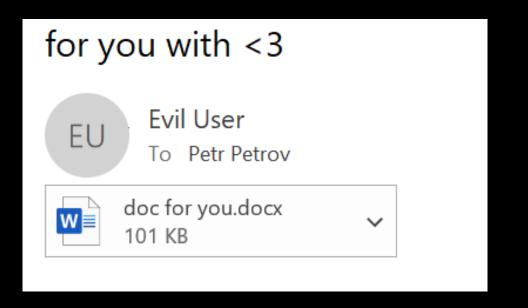
Allow Macros – need for AIP work. So you can't work without Allow Macros

Malicious Doc



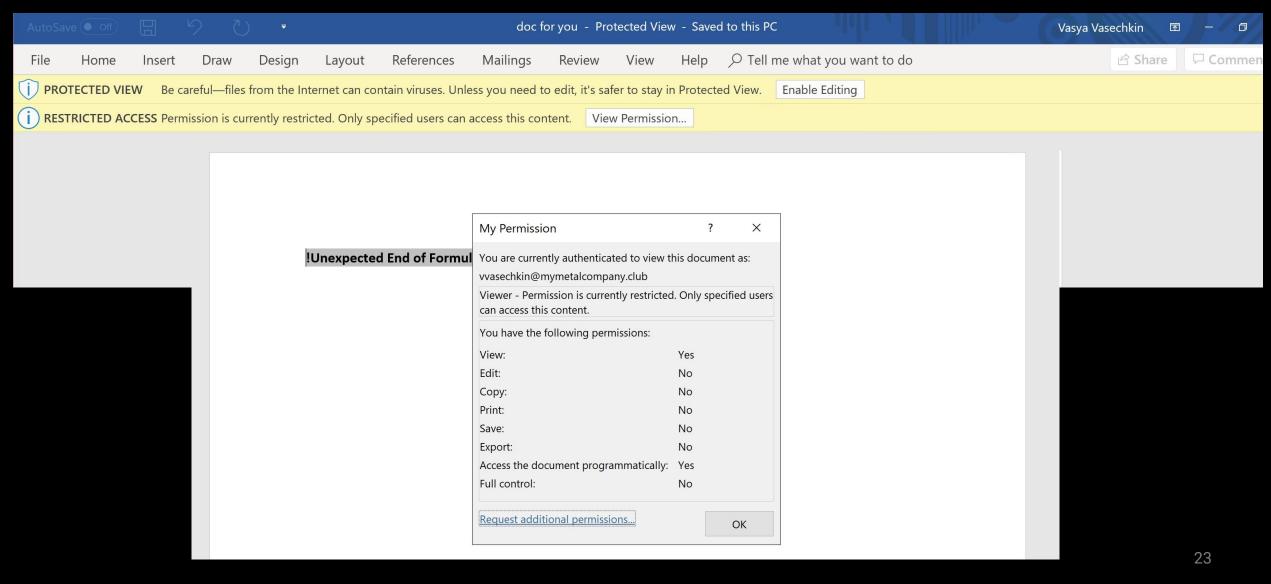






Vasechkin & Malicious Doc





Vasechkin & Malicious Doc



Microsoft Word



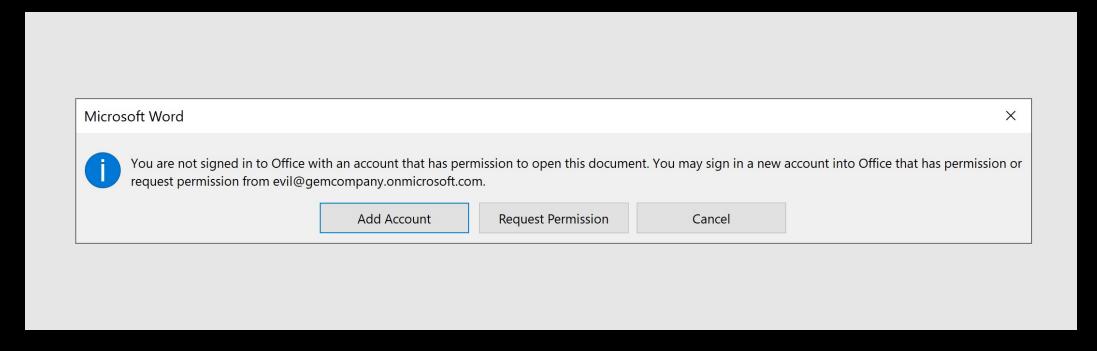
Sorry, Word can't open this document because it's protected by Information Rights Management (IRM). To view this document please open it in Microsoft Word.

Your feedback helps Microsoft improve Word. <u>Give</u> feedback to Microsoft

User can open the document in Word only

Petrov & Malicious Doc

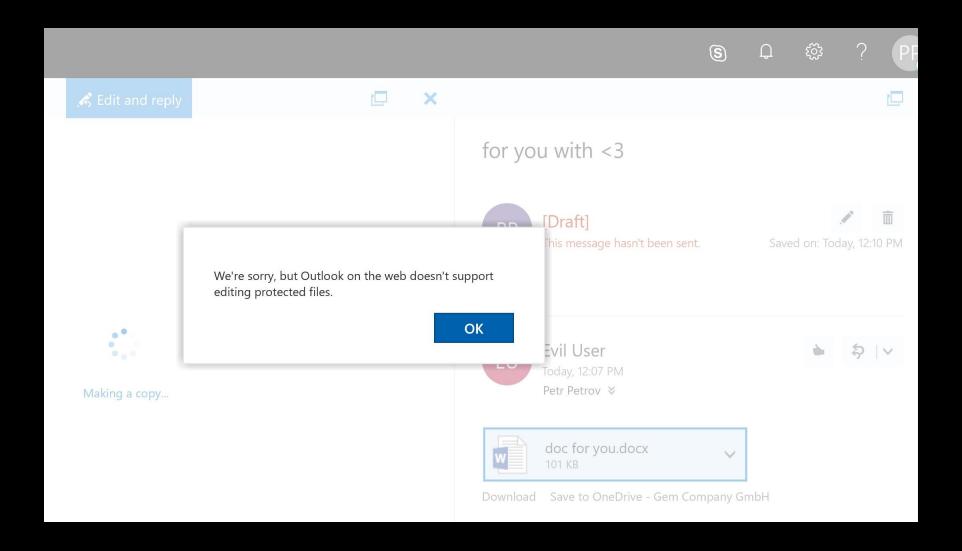




User can see real account email But can't open document

Petrov & Malicious Doc





Track Malicious Doc



Summ	nary List Timeline Map	o Settings		
	Name		Status	Date 🗸
<u>*</u>	Vasya Vasechkin		Viewed	12:53 PM
<u>*</u>	Petr Petrov		Denied	12:11 PM

Email notifications Notify me by email when someone tries to open this document Notify me only when access to the document is denied Don't notify me

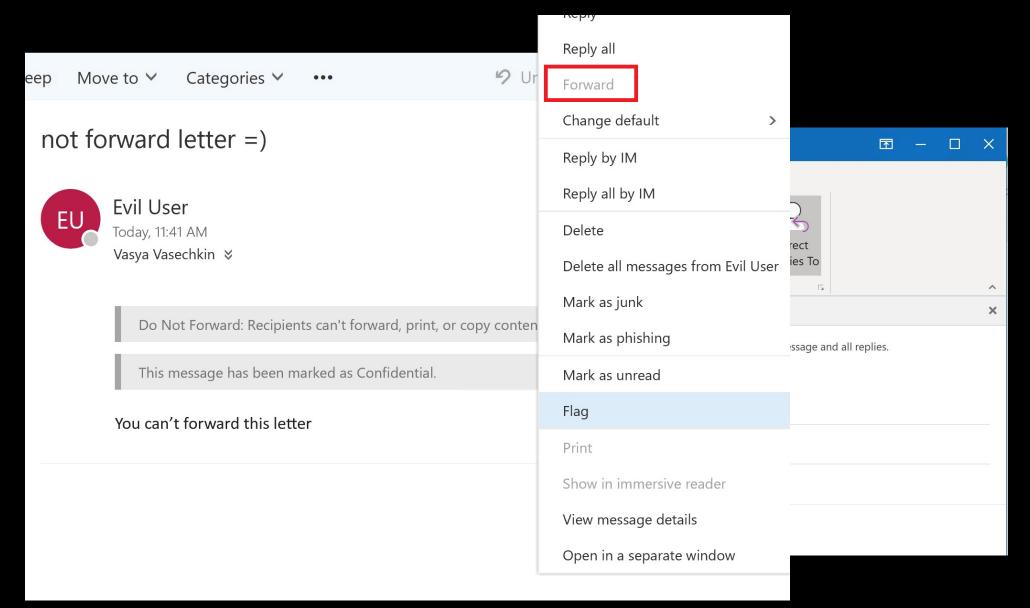
ppetrov@mymetalcompany.club was denied access to doc for you.docx

ppetrov@mymetalcompany.club was denied access to doc for you.docx on 2019 13:27 UTC.

View detailed tracking information for this document.

#DoNotForward





#DoNotForward



for Vasechkin only



Evil User

To Vasya Vasechkin

i Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.

Permission granted by: evil@gemcompany.onmicrosoft.com



doc for you.docx 58 KB



All Employees







Evil User

To Vasya Vasechkin

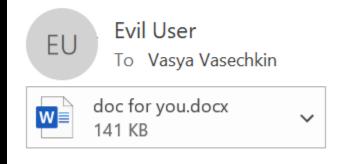
i Highly Confidential \ All Employees - Highly confidential data that allows all employees view, edit, and reply permissions to this content.

Data owners can track and revoke content.

Permission granted by: evil@gemcompany.onmicrosoft.com



new for you



Microsoft detected the malicious documents

Results



- We can use Azure Information Protection for phishing companies
- But we can use only protection for customer permission
- Azure Information Protection helps us to understand users action (who and when opened document)

Our contacts

- email: mis@m13.su
- Telegram channel: @mis_team
- Github: mis-team



tHandler):



i shanaka t

-

301 Vall - V

do Cer

16 17

see do estab

r, info

-

tests