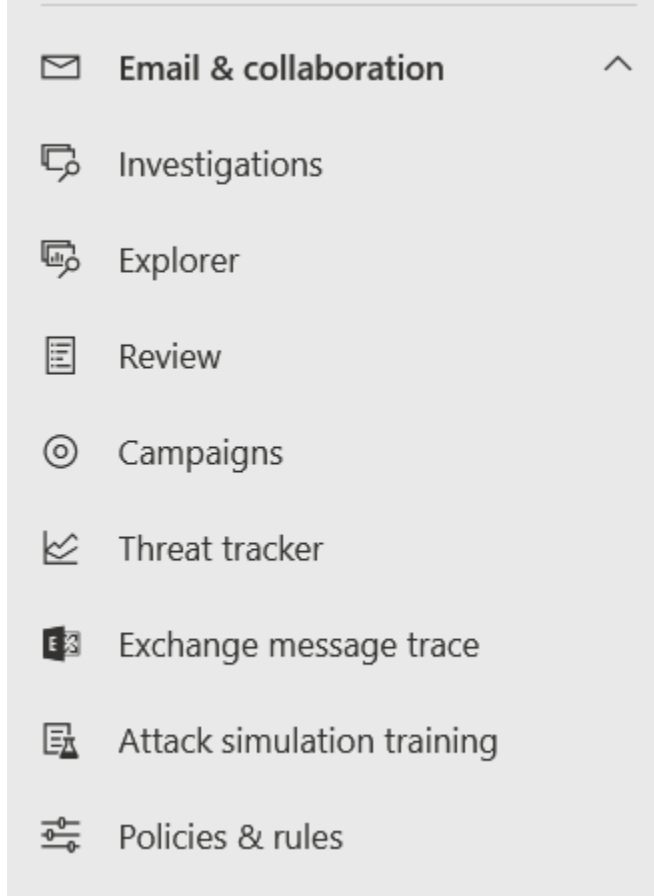


E-mail & Collaboration - Threat Explorer Nedir ?

[Microsoft Security Portal](#) 'a girdiğimizde sol menüde bir çok kaynak ile karşılaşmaktayız. Bu menüde bulunan ve **Microsoft Defender for Office 365** menüsünü barındıran **E-mail & Collaboration** başlığı bulunmakta.



E-mail & Collaboration başlığı altında M365 uygulamalarında gerçek zamanlı olarak izlememizi, yönetmemizi ve takip etmemizi sağlayan alt menülerle karşılaşmaktayız. Bugün alt menülerden biri olan **Explorer** menüsünü inceleyeceğiz.

Threat Explorer Yetki Gereksinimleri

Threat Explorer ekranına ulaşabilmek ve işlem gerçekleştirebilmek için aşağıdaki rollerden birine ihtiyaç duymaktasınız.

- Global Administrator
- Organization Management
- Security Administrator

- Security Reader (Sadece görüntüleme yetkisi içerir)

Threat Explorer

Explorer

[Learn more](#) [Chart View](#) [New version](#)

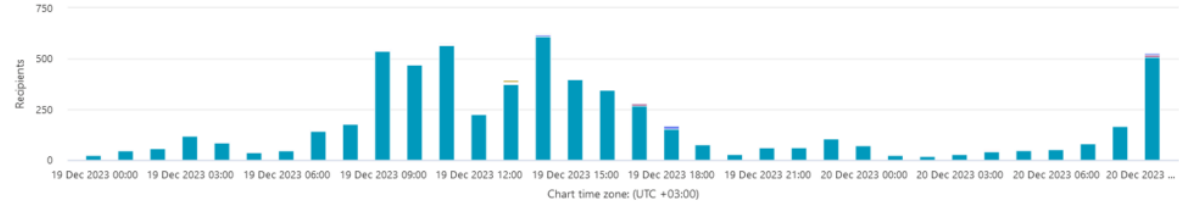
[All email](#) [Malware](#) [Phish](#) [Campaigns](#) [Content Malware](#) [URL clicks](#)

[2023-12-19 00:00 - 2023-12-20 23:59](#) [Sender](#) [Equal any of](#) [Use commas \(,\) to separate multiple entries...](#) [Refresh](#) [AND](#)

[Save query](#)

[Delivery action](#)

[Export chart data](#)



[Delivered](#) [Delivered to junk](#) [Delivered to deleted folder](#) [Blocked](#)

[Email](#) [URL clicks](#) [Top URLs](#) [Top clicks](#) [Top targeted users](#) [Email origin](#) [Campaign](#)

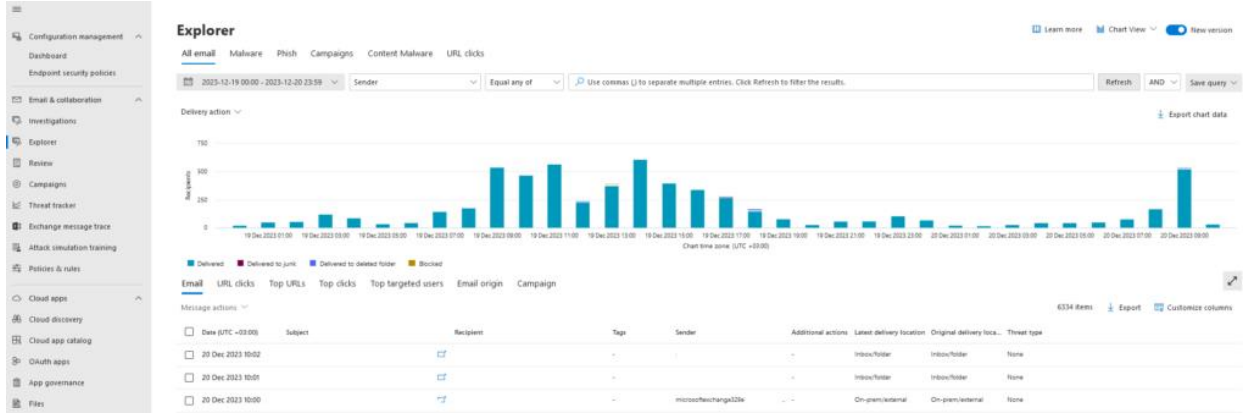
[Message actions](#)

6292 items [Export](#) [Customize columns](#)

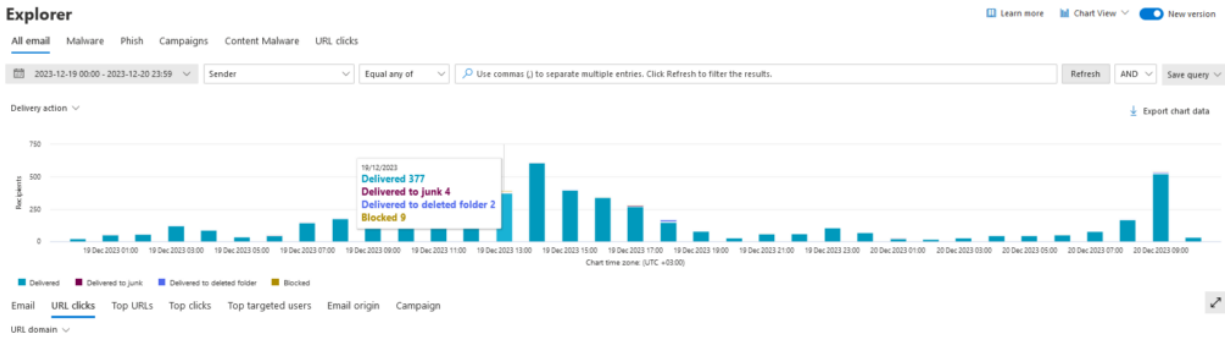
[Date \(UTC +03:00\)](#) [Subject](#) [Recipient](#) [Tags](#) [Sender](#) [Additional actions](#)

Güvenlik Operasyonları ekiplerinin Microsoft Defender portalındaki tehditleri araştırmasına ve bunlara yanıt vermesine yardımcı olan güçlü, gerçek zamanlı bir araçtır. Explorer (ve gerçek zamanlı algılama raporu), e-postalarda ve Office 365'teki dosyalardaki şüpheli kötü amaçlı yazılım ve kimlik avı hakkındaki bilgilerin yanı sıra kuruluşunuza yönelik diğer güvenlik tehditleri ve riskleri hakkında bilgileri görüntüler. Tüm trafiği görebildiğiniz tehditleri izleyebildiğiniz Gerçekleşmiş olan tehditlerin detaylı incelenebildiği alanlara yönlendiren bir mekanizmaya sahiptir. Bununla birlikte, son kullanıcılar bu tehditler özelinde yapmış oldukları davranışları izlemenizi de sağlamaktadır.

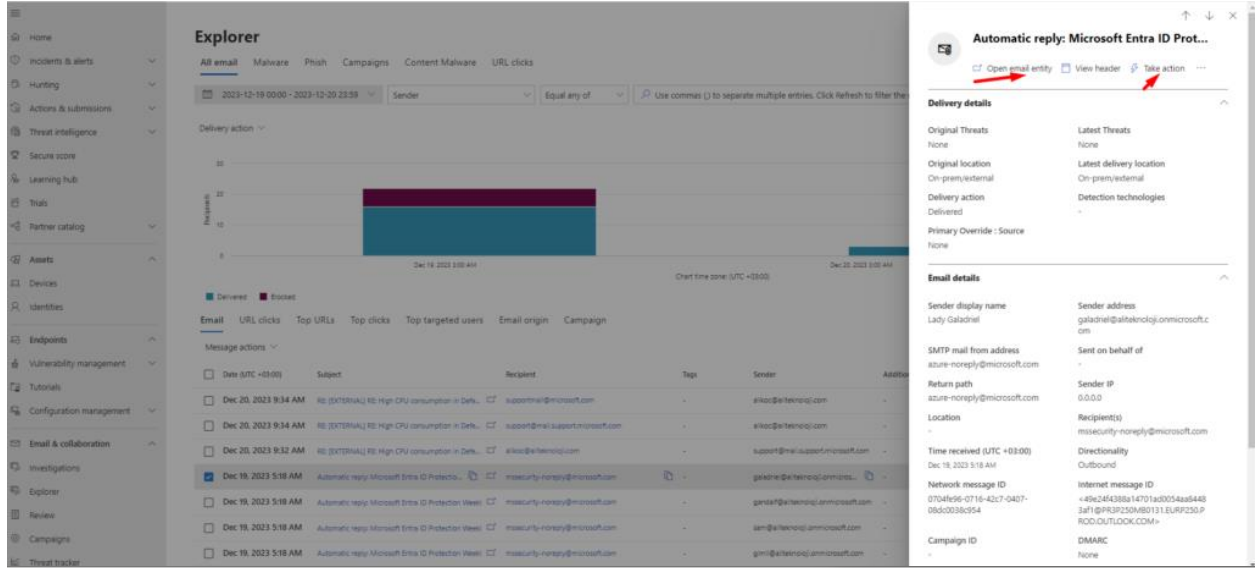
Explorer'ı ilk açtığınızda, varsayılan görünüm son 7 güne ait e-postadaki kötü amaçlı yazılım algılamalarını gösterir. Bu rapor aynı zamanda Güvenli Bağlantılar tarafından algılanan kötü amaçlı URL'ler ve Güvenli Ekler tarafından algılanan kötü amaçlı dosyalar gibi Office 365 için Microsoft Defender algılamalarını da gösterebilir. Bu rapor, son 30 güne ait verileri gösterecek şekilde değiştirilebilir (Office 365 P2 için Microsoft Defender ücretli aboneliğiyle). Deneme abonelikleri yalnızca son yedi güne ait verileri içerecektir.



Explorer menüsünde ana ekrana baktığımızda, **All email** başlığı altında, tüm tehdit içeren (Malware, Phishing.....) mailleri görüntülemekteyiz. Bu görünüm, kimlik avı veya kötü amaçlı yazılım nedeniyle kötü amaçlı olarak tanımlanan e-postaların yanı sıra normal e-posta, spam ve toplu posta gibi kötü amaçlı olmayan diğer tüm e-postaları gösterir. Burada saat bazlı olarak görüntülediğimiz grafik ile gelen mailler üzerinden alınan aksiyonları da görüntüleyebiliriz.



Ayrıca alt menüde bulunan maillere tıkladığınızda o mail ile ilgili tüm detaylara ulaşabileceğiniz bir ekran sizlerle paylaşılmaktadır. Bu ekranda bulunan **Open email Entity** ekranına giderek detaylı inceleme yapabilir, **Take action** menüsünden gelen tehdit hakkında aksiyon alabilirsiniz.



Take action

- ☒ Choose actions
- ☐ Choose target entities
- ☐ Review and submit

Choose response actions

Specify the actions you want to take. Only actions applicable to the selected entity are available. We've grayed out the actions that aren't relevant to you.

Email message actions

- ☐ Move to mailbox folder
- ☐ Submit to Microsoft for review
- ☐ Initiate automated investigation
- ☐ Propose remediation
Create admin request for remediation actions


Next

Cancel

En çok Hedeflenen Kullanıcılar

Gerçekleşen saldırılarda, en çok hedef alınan kullanıcıları görebilir ve bu doğrultuda aksiyonlar alabilirsiniz.

Ayrıca, Hedeflenen kullanıcıların listesini, 3.000 sınırına kadar dışa aktarabileceksiniz. Attempts seçeneğini seçtiğinizde (örneğin, aşağıdaki resimde 13 attempts), Threat Explorer'nde filtrelenmiş bir görünüm açılacaktır; böylece söz konusu kullanıcıya yönelik e-postalar ve tehditler arasında daha fazla ayrıntı görebilirsiniz.

Email	URL clicks	URLs	Top targeted users	Email origin	Campaign
Top targeted users				↓ Export	
SE	secre			13 attempts	
TI	tifc@			3 attempts	
DA	davie			1 attempts	
SU	sumi			1 attempts	

URL Click ve Dışarı Aktarma

Tehdit olarak iletilmiş olan URL'lere tıklanma raporlarını görüntüleyebilir ve dışarı aktarabilirsiniz.

Email	Clicks	Details	↓ Export	
Click Time (UTC)	User	Network Message ID	Click Verdict	
10/3/19 8:30 PM	tifc@o365tisdfv2.onmicrosoft.com	-45af-08d745d93ff1	Blocked	
10/4/19 1:00 AM	tifc@o365tisdfv2.onmicrosoft.com	fca7ee8a 2a10 4787	Blocked	

Filter menüsünden , detaylı olarak arama yapılabilir ve ilgili mail ile çalışma yapılabilir.

Explorer is a powerful, near real-time tool to help Security Operations teams investigate and respond to threats in the Security & Compliance

View [All email](#)

This view shows information about all email messages sent by external users into your organization, or internal email sent between your users the view for threat hunting, and you can export up to 200,000 records for offline analysis. [Show more](#)

Save query

Save query as

Saved query settings

Export

Alert ID

372c9b5b-a6c3-5847-1800-08d8b6773639

Refresh

Advanced filter

Alert ID : 372c9b5b-a6c3-5847-1800-08d8b6773639

2020-12-13

03:00

Basic

Sender

Recipients

Recipient domains

Sender domain

Subject

Return path

Return path domain

Malware family

Tags

Exchange transport r...

Context

Connector

Delivery action

Additional action

Directionality

Detection technology

Original delivery loc...

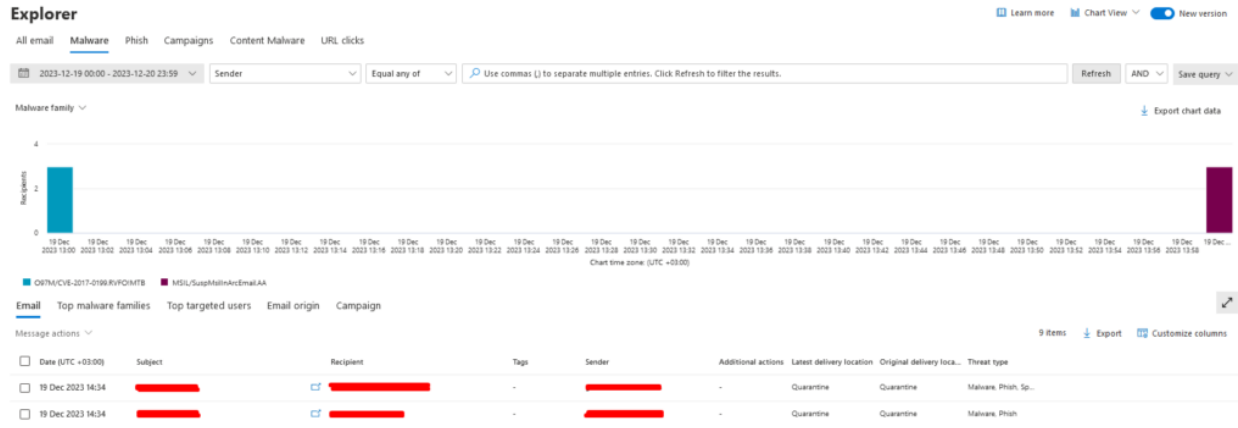
Latest delivery locati...

Üst menüde bulunan diğer başlıkları incelediğimizde, ilk ekranda gördüğümüz tüm mailleri kapsayan spesifik olarak sınıflandırdığımız alanları görüntülüyor olacağız.

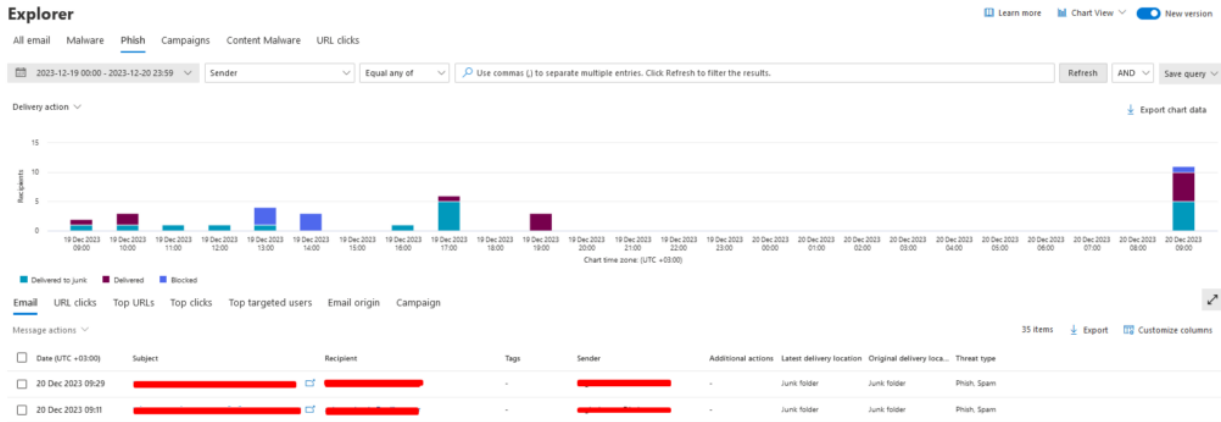
Explorer

All email Malware Phish Campaigns Content Malware URL clicks

Malware, Phish, Campaigns , Content Malware ve URL Clicks menülerinde tüm detayları ve tehditleri farklı sınıflarda inceleyebildiğimiz alanlara mevcuttur.



Alt menüde detaylarını gördüğümüz maillerin Threat Type , delivery location gibi detaylarına ulaşabilir, ayrıca subject menüsünden mail detaylarına tıklayarak detaylı analiz yapılabilir.



Phish menüsü altında, phishing olarak algılanan mailleri ve detaylarını inceleyebiliriz.

Explorer

All email Malware Phish Campaigns Content Malware URL clicks

Learn more Chart View New version

2023-12-19 00:00 - 2023-12-20 23:59 Campaign Type Equal any of Select an option Refresh AND Save query

Campaign Type

Export chart data



Malware

Campaign Campaign origin

Note: Campaigns include a specific subset of messages. [Learn more](#)

2 items Export Customize columns

Name	Sample subject	Targeted	Type	SubType	Tags	Recipients	Inboxed	Clicked	ClickRate	Visited
<input type="checkbox"/> Malware.998250AE	[REDACTED]	0.0%	Malware	PHG/Phish/POBT...	-	3	0	0	-	0
<input type="checkbox"/> Malware.A50CD9FE	[REDACTED]	0.1%	Malware	MSL/SuspMalware...	-	3	0	0	-	0

Explorer

All email Malware Phish Campaigns Content Malware URL clicks

2023-12-19 00:00 - 2023-12-20 23:59 Campaign Type Equal any of Select an option

Campaign Type

No data to show
There are no results for the selected filters. Please update again.

Campaign Campaign origin

Note: Campaigns include a specific subset of messages. [Learn more](#)

Name	Sample subject	Targeted	Type
<input checked="" type="checkbox"/> Malware.998250AE	[REDACTED]	0.0%	Malware
<input type="checkbox"/> Malware.A50CD9FE	[REDACTED]	0.1%	Malware



Malware.998250AE - [REDACTED]
Campaign ID 998250AE.10208461.83DF1579.CFA59163.20105.MALWARE
Active 1234 min(s) ago

Impact **Blocked** Messages 3 Inboxed 0 Clicked link 0 Visited link 0 Targeted(%) 0
Tue Dec 19 2023 13:00 13:00 - Tue Dec 19 2023 13:00 13:00 Refresh



Sender (IP)	Sender domains	Filter verdicts	Message destination
190.224.163.164	ageim-motor.com.tr	Detected	Quarantine

URL clicks Sender IPs Senders Attachments URLs

Do you think this campaign has accurately grouped these messages together? Yes No

Explore messages Download threat report

Campaigns menüsü altında, maruz kalınan olan malware ve detaylı çalışma analizine erişebilirsiniz.

Content Malware ekranı altında , Microsoft Defender for Office 365 tarafından kötü amaçlı olarak tanınan dosyaları görüntülemekteyiz.

Explorer

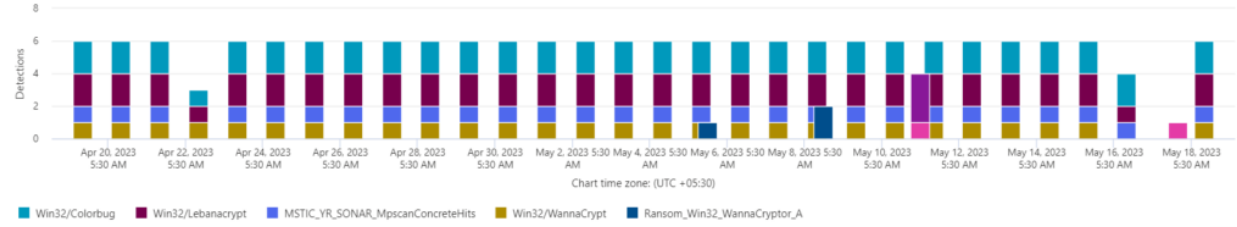
Learn more Chart View New version

All email Malware Phish Campaigns Content Malware URL clicks

2023-04-20 00:00 - 2023-05-19 23:59 File name Equal any of Use commas (,) to separate multiple entries. Click Refresh to filter the results. Refresh AND

Malware family

Export chart data



Document

URL Clicks ekranından, son kullanıcıların maruz kaldığı ataklarda almış oldukları aksiyonu görüntüleyebiliriz.

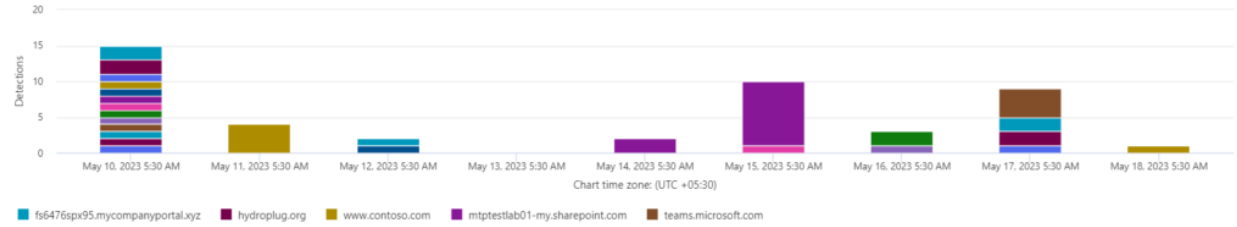
Explorer

Learn more New version

All email Malware Phish Campaigns Content Malware URL clicks

2023-05-10 00:00 - 2023-05-19 23:59 Recipients Equal any of Use commas (,) to separate multiple entries. Click Refresh... Refresh AND Save query

URL domain



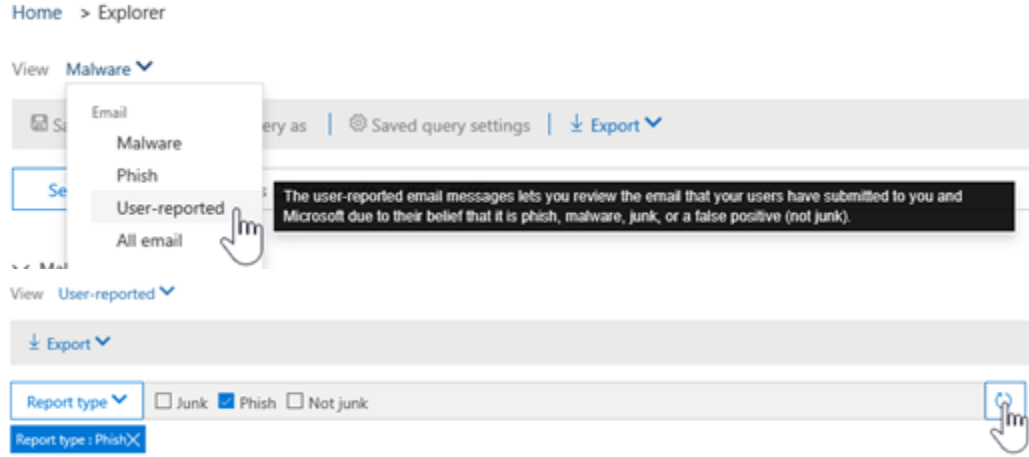
Results Top clicks Top targeted users

Results Top clicks Top targeted users

26 items Export top clicks View all clicks Customize columns

URL	Blocked	Allowed	Block overridden	Pending verdict	Pending verdict bypassed
<input type="checkbox"/> mtptestlab01-my.sharepoint.com/w/g/personal/jenny...	-	8	-	-	-
<input type="checkbox"/> www.contoso.com/	-	4	-	-	-
<input type="checkbox"/> teams.microsoft.com/l/meetup-join/19%3ameeting_Nz...	-	3	-	-	-

Son kullanıcılar tarafından bizlere bildirilen emaiları Threat Explorer başlığı altından inceleyebiliriz.



Tüm bu detayları göz önüne aldığımızda;

Microsoft Defender for Office 365 Threat Explorer ekranı bizlere Gerçek Zamanlı algılamalar, güvenlik operasyonları ekibinizin tehditleri verimli bir şekilde araştırmasına ve bunlara yanıt vermesine yardımcı olmaktadır. Hem zamandan hem de efordan tasarruf etmesini sağlayan ve detaylı analizleri yaparak kurum güvenliğinin sağlanmasını hedeflemektedir.