CLOUD OFFICE SECURITY

MICROSOFT 365 İÇİN GÜÇLENDİRİLMİŞ GÜVENLİK

Dünya genelinde milyonlarca şirket günlük operasyonlarını buluta taşıyor. Windows en popüler platform olmaya devam ettiği için bu şirketlerin çoğunun Microsoft 365 uygulamalarını kullanmaya karar vermesi gayet doğal. Microsoft'un güvenliğe yatırım yapmasına rağmen, birçok tehdit halen çatlaklardan sızmayı başarıyor.

İşte, ESET Cloud Office Security bu aşamada devreye girerek Microsoft 365 uygulamalarına ek koruma katmanları sağlıyor.

ECOS'un algılama teknolojisi, ESET'in 30 yıllık tehditle mücadele deneyimine ve gelişimine dayanır ve güvenilir spam filtreleme, kimlik avı önleme ve zararlı yazılım koruması sağlar. Exchange, OneDrive, SharePoint ve Teams'de algılanan şüpheli etkinlikler, kullanımı kolay bir bulut konsolu aracılığıyla hemen güvenlik personeline bildirilir.

ESET CLOUD OFFICE SECURITY TESPİTLERİNDEN BAZILARI

ESET Cloud Office Security, sadece 2021'in ilk yarısında Microsoft 365'te bulunan yerel korumayı atlayan binlerce çeşitli tehdidi engelledi. Çoğunluğu kimlik avı ve spam mesajları iken, infostealers, downloaders ve diğer tehlikeli kötü amaçlı yazılım türleri de tespit edildi. En ciddi tehditlerden bazıları aşağıda açıklanıyor.

İndiriciler

Emotet

PowerShell/ TrojanDownloader.Agent'ın bir varyantı olarak algılandı

Emotet, öncelikle bankacılık truva atları, infostealers ve fidye yazılımları gibi daha fazla zararlıyı indirmek için kullanılan kötü şöhretli, modüler bir truva atıydı. Ocak 2021'de piyasaya sürülmeden önce, kötü amaçlı Office ve PDF belgeleri içeren büyük ölçekli malspam kampanyaları başlatarak, Ryuk, Conti, BitPaymer ve DoppelPaymer gibi en vicdansız fidye yazılımı ailelerinden bazılarını yayarak en büyük ve en üretken botnet'lerden birini oluşturmuştu.

Detaylı bilgi

Nemucod

JS/TrojanDownloader.Nemucod ve JS/ Danger.ScriptAttachment varyantları olarak algılandı

Nemucod, e-postalardaki kötü amaçlı ekler aracılığıyla yayılan kötü şöhretli bir indirici ailesidir. Ana amacı, etkilenen cihaza daha fazla kötü amaçlı yazılım indirmektir. Bu kötü amaçlı yazılım ailesi geçmişte birçok büyük ölçekli malspam kampanyalarını körükledi, özellikle TrickBot gibi botnet'leri dağıtan veya GandCrab veAvaddon fidye yazılımı gibi son yükü teslim edenleri.

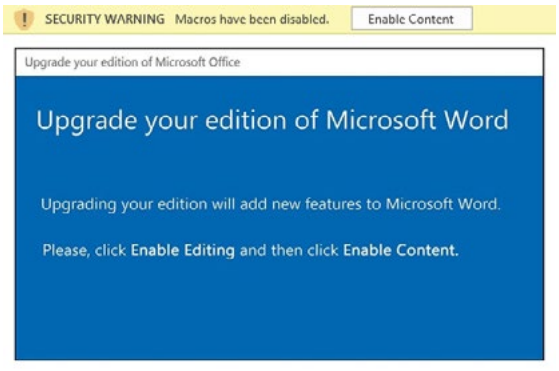
Detaylı bilgi

Bulaşıcı VBA makroları

VBA/TrojanDownloader.Agent varyantları olarak algılandı

VBA/TrojanDownloader.Agent, genellikle riskli Microsoft Office dosyalarına eklenmiş zararlı makroları kapsayan bir algılamadır. Bunlar, spam kampanyalarına eklenir ve alıcıyla ilgili önemli bilgiler içeriyormuş gibi gönderilir. Kurban tarafından etkinleştirilirse, zararlı makro ek zararlılar indirir ve yürütür. Bu teknik, Qbot, Trickbot, Dridex ve Emotet dahil olmak üzere birden fazla indirici ve botnet ailesi tarafından kullanılır.

Detaylı bilgi



Artık geçersiz olan Emotet botnet tarafından zararlı makroları yaymak için kullanılan belge şablonları

Bilgi Hırsızları

Agent Tesla

MSIL/Kryptik ve MSIL/GenKryptik varyantları olarak algılandı

Agent Tesla, hizmet olarak kötü amaçlı yazılım iş modeli ve kullanımı kolay arayüzü nedeniyle son derece popüler hale gelen bir uzaktan erişim truva atıdır. Bu güçlü zararlının özellikleri arasında çeşitli kimlik bilgilerini depolayan uygulamalardan giriş bilgilerinin toplanması, keylogging ve kurbanın masaüstünün ekran görüntülerinin alınması yer alıyor. Genellikle malspam yoluyla yayılır, dağıtım için meşru, saldırıya uğramış e-posta hesaplarını kötüye kullanarak. Algılamadan kaçmak için karmaşık teknikler kullanır.

Detaylı bilgi

Win32/Agent.ADAT trojan

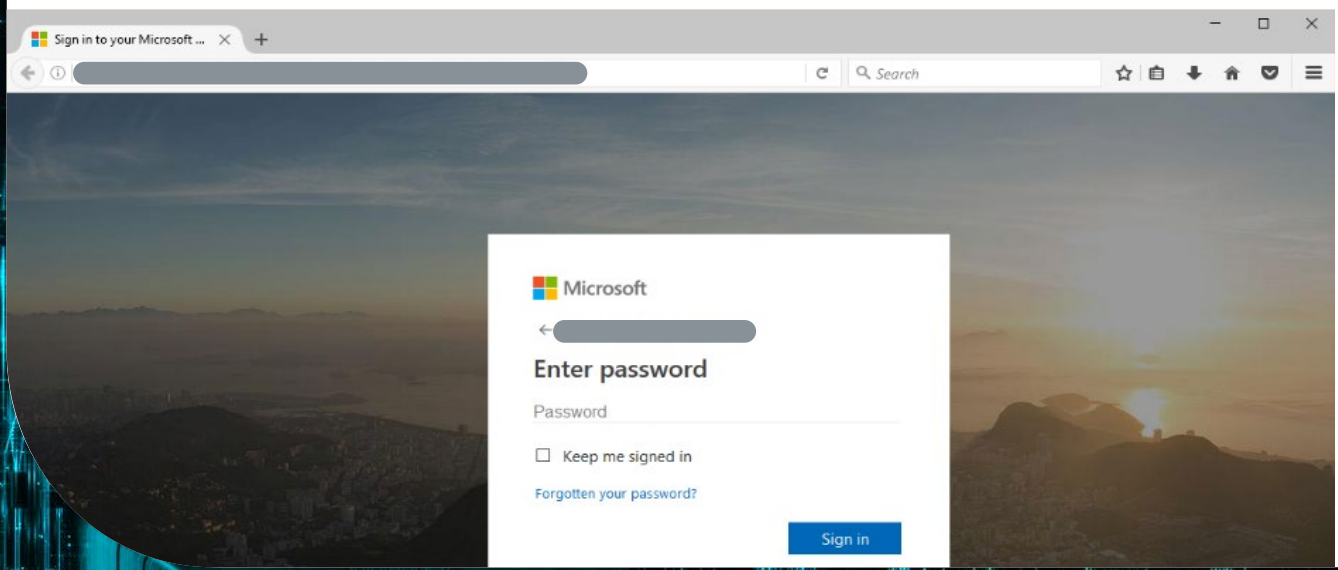
Win32/Agent.ADAT, "tax_invoice.com" adlı bir dosyanın algılama adıdır. Bu dosya, finansal hile kullanarak diğer birkaç zararlı dosyayı daha indirir ve kurbanın bilgisi olmadan yürütür. Zararlı yürütülebilir dosyalardan birinin içindeki kod, diğer bulaşmaların ilk aşaması olan bir işlem için zemin hazırlar. Formbook'un yük olarak kullanıldığı durumlarda da benzer bir saldırı yolu görülmüştür. Formbook kötü amaçlı yazılım ailesinin birincil amacı, tarayıcı geçmişi ve depolanan şifreler gibi hassas bilgileri toplamak ve çalmaktır.

Formbook hakkında detaylı bilgi

Kimlik Avı

HTML/Phishing.Microsoft

HTML/Phishing.Microsoft, çoğunlukla e-posta eki olarak dağıtılan bir kimlik avı tehdidinin algılamasıdır. Saldırganlar, dosyanın kötü amacını gizlemek için ödenmemiş faturalar ve ödeme emirleri hilelerini kullanır veya mağdurları "Yeni Faks Alındı" veya "Sesli Mesaj" gibi ilgi çekici dosya adlarıyla cezbetmeye çalışır. Ek açıldıktan sonra, kurbanlar Office 365 kimlik bilgilerini toplamak için tasarlanmış sahte bir oturum açma web sitesine yönlendirilir.



ESET Cloud Office Security

Kullanımı kolay bir bulut yönetim konsolu aracılığıyla Microsoft 365 uygulamaları için kötü amaçlı yazılım, spam ve kimlik avı saldırılarına karşı gelişmiş önleyici koruma.

DETAYLI BİLGİ

ESET Hakkında

ESET® 30 yılı aşkın bir süredir sektör lideri BT güvenlik yazılımları ve hizmetleri geliştirerek dünya çapındaki işletmeler ve tüketiciler için gelişen siber güvenlik tehditlerine karşı anında ve kapsamlı koruma sunmaktadır.

ESET özel sektöre aittir. Borçsuz ve kredisiz, tüm müşterilerimizin nihai koruması için yapılması gerekenleri yapma özgürlüğüne sahibiz.

www.eset.com.tr

ESET IN NUMBERS

110m+	400b+	200+	13
küresel kullanıcı	kurumsal müşteri	ülke & bölge	ARGE merkezi

CYBERSECURITY
EXPERTS ON YOUR SIDE