**Emotet kötü amaçlı yazılım kullanımı üç ayda yüzde 3 bine yakın arttı!**

**HP Wolf Security'nin en son yayımladığı Güvenlik Tehdidi Öngörüleri Raporu, bu yılın ilk çeyreğinde siber tehditlerde yüzde 27'lik genel bir artış olduğunu ortaya koydu. Saldırganlar, 545 farklı kötü amaçlı yazılım ailesi kullanırken bu yazılımlar içerisinde Emotet, AgentTesla ve Nemucod ilk üç sırada yer aldı. Emotet kötü amaçlı spam saldırılarda artış oranı yüzde 2 bin 823’ü buldu.**

HP, 2022'nin 1. çeyreğinde siber tehditlerde yüzde 27'lik genel bir artış olduğunu ve HP Wolf Security tehdit araştırma ekibinin Emotet kötü amaçlı spam saldırılarda 2021'in 4. çeyreğine kıyasla 28 kat (yüzde 2.823) artış tespit ettiğini duyurdu. Gerçek dünyadaki siber güvenlik saldırılarının analizini ortaya koyan en son küresel [HP Wolf Güvenlik Tehditleri Öngörü Raporu](https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q1-2022/), Emotet'in 36 basamak yükselerek bu çeyrekte tespit edilen en yaygın kötü amaçlı yazılım ailesi olduğunu gösteriyor (saptanan tüm kötü amaçlı yazılımların yüzde 9'unu temsil ediyor). Kullanıcıların PC'lerine bulaşmayı kolaylaştırmak için e-postaları ele geçiren ve Japon kurumlarını hedef alan Emotet saldırılardan biri, tespit edilen XLSM (Microsoft Excel) kötü amaçlı yazılımların önceki çeyreğe kıyasla yüzde 879'luk artışına neden oldu.

HP Wolf Security güvenlik yazılımının kuruluğu olduğu ve çalıştığı milyonlarca cihazdan elde edilen verilere dayanıyor. HP Wolf Security, kullanıcıyı korumak ve denenmiş tüm bulaşma zincirini anlayıp yakalamak için izole edilmiş, mikro sanal makinelerde (mikro VM'ler) riskli görevler açarak kötü amaçlı yazılımları izliyor ve diğer güvenlik araçlarını aşan tehditleri azaltıyor. HP müşterileri bugüne kadar 18 milyardan fazla e-posta ekine, web sayfasına, indirme butonuna tıkladı ve bunların hiçbirinde ihlal yaşanmadı.[[1]](#endnote-1) Bu veriler, tehdit aktörlerinin kötü amaçlı yazılımları nasıl kullandıklarına dair benzersiz bilgiler sağlıyor.

Rapordaki diğer önemli bulgular arasında şunlar yer alıyor:

* Tehditlerin yüzde 9'unun HP Wolf Security tarafından izole edilmeden önce tespit edilemediği görüldü. HP Wolf Security tarafından izole edilmiş e-posta kötü amaçlı yazılımlarının yüzde 14'ünün ise en az bir e-posta ağ geçidi tarayıcısını atlattığı tespit edildi.
* Diğer güvenlik araçlarının hash bilgilerini kullanarak tehditleri tespit etmesi ortalama 3 günden (79 saat) fazla sürdü.
* HP Wolf Security tarafından izole edilen kötü amaçlı yazılımların yüzde 45'i Office dosyaları biçimindeydi.
* Saldırganlar, kurumlara virüs bulaştırma girişimlerinde 545 farklı kötü amaçlı yazılım ailesi kullandı. Bu yazılımlar içerisinde Emotet, AgentTesla ve Nemucod ilk üç sırada yer aldı.
* Bir Microsoft Denklem Düzenleyicisi istismarı (CVE-2017-11882), yakalanan tüm kötü amaçlı örneklerin yüzde 18'ini oluşturuyordu.
* Tespit edilen kötü amaçlı yazılımların %69'u e-posta yoluyla bulaşırken web indirmeleri yüzde 18'inden sorumluydu. Kötü amaçlı yazılım bulaştırmak için en çok ekli belgeler (yüzde 29), arşivler (yüzde 28), yürütülebilir dosyalar (yüzde 21), elektronik tablolar (yüzde 20) kullanıldı.
* Kötü amaçlı yazılımları dağıtmak için kullanılan en yaygın ekler arasında elektronik tablolar (yüzde 33), yürütülebilir dosyalar ve komut dosyaları (yüzde 29), arşivler (yüzde 22) ve belgeler (yüzde 11) yer aldı.
* En yaygın kimlik avı yolları; sipariş, ödeme, satın alma, istek ve fatura gibi ticari işlemlerdi.

HP Wolf Security tehdit araştırma ekibinden Kıdemli Kötü Amaçlı Yazılım Analisti Alex Holland konuyla ilgili açıklamasında, "1. çeyrek verilerimiz, 2021'in başlarında bu saldırıların önünün kesilmesinden bu yana geçen sürede gördüğümüz en büyük Emotet faaliyetine işaret ediyor. Burada Emotet operatörlerinin yeniden toplandığına, güçlerini geri kazandığına ve botnet'i büyütmeye yatırım yaptığına dair açık bir işaret görüyoruz. Emotet bir [zamanlar CISA tarafından](https://www.cisa.gov/uscert/ncas/alerts/TA18-201A) en yıkıcı ve maliyetli kötü amaçlı yazılımlardan biri olarak tanımlanmıştı. Emotet operatörleri genellikle fidye yazılımı gruplarıyla iş birliği yapıyor; bu modeli devam ettireceklerini düşünüyoruz. Bu yüzden yeniden ortaya çıkmaları hem işletmeler hem de kamu sektörü için kötü bir haber.” dedi.

HP Kişisel Sistemler Küresel Güvenlik Başkanı Dr. Ian Pratt ise “Bu çeyrekte HP Wolf Security tarafından tespit edilen tehditlerde yüzde 27 gibi önemli bir artış oranı görüyoruz. Siber suçlular BT ortamındaki değişikliklere karşılık olarak yaklaşımlarını değiştirdikçe saldırıların hacmi ve çeşitliliği artmaya devam ediyor ve geleneksel araçların saldırıları algılaması zorlaşıyor. Algılamayı atlamak için kullanılan alternatif dosya türleri ve tekniklerindeki gelişmeler nedeniyle kurumların rotasını değiştirmesi ve uç nokta güvenliğine katmanlı bir yaklaşım benimsemesi gerekiyor. En azından ayrıcalık ilkesini uygulayarak ve en yaygın tehdit kaynaklarını (e-postadan, tarayıcılardan veya indirmelerden) izole ederek bu kaynaklar aracılığıyla bulaşan kötü amaçlı yazılımlar zararsız hale getirilmeli. Bu şekilde, kurumların siber tehditlere maruz kalma riski önemli ölçüde azalacaktır." açıklamasında bulundu.

**İlgili Kişiler**Ceren Moral – Bordo PR  
0533 921 43 53  
[cerenm@bordopr.com](mailto:cerenm@bordopr.com)

Beril Pelesen – Bordo PR  
0537 220 49 39  
[berilp@bordopr.com](mailto:berilp@bordopr.com)

**HP Hakkında**

HP Inc., düşünceli bir fikrin dünyayı değiştirme gücüne sahip olduğuna inanan bir teknoloji şirketidir. Kişisel sistemler, yazıcılar ve 3D baskı çözümlerinden oluşan ürün ve hizmet portföyü, bu fikirlerin hayata kazandırılmasına yardımcı olmaktadır. [http://www.hp.com](http://www.hp.com/)

**HP Wolf Security Hakkında**

HP Wolf Security, uç nokta güvenliğinin yeni bir türüdür. HP'nin donanım tarafından zorlanan güvenlik ve uç nokta odaklı güvenlik hizmetleri portföyü, kurumların bilgisayarları, yazıcıları ve insanları siber avcılardan uzak tutmasına yardımcı olmak için tasarlanmıştır. HP Wolf Security, donanım düzeyinde başlayıp yazılım ve hizmetlere yayılan kapsamlı uç nokta koruması ve esnekliği sağlamaktadır.[[2]](#endnote-2)

1. Varsayımlar, HP'nin müşteri tarafından bildirilen verilere ve kurulu tabana ilişkin dahili analizine dayanmaktadır. [↑](#endnote-ref-1)
2. HP Security artık HP Wolf Security olarak adlandırılmaktadır. Güvenlik özellikleri platforma göre değişiklik gösterir, ayrıntılar için lütfen ürün veri sayfasına bakınız. [↑](#endnote-ref-2)