|  |
| --- |
| **BASIN BÜLTENİ**  **HP, kullanıcıları kandırma konusunda giderek daha da ustalaşan siber suçluların yeni alanlara sıçradığını tespit etti**  **Gizli teknikler ve büyüyen kötü amaçlı Excel yazılımı saldırıları, kullanıcıları fidye yazılımı çetelerinin hedefine koyuyor.** |

HP Inc. (NYSE: HPQ) algılama araçlarından kaçan ve kullanıcı uç noktalarına ulaştırılan tehditleri yalıtarak, siber suçlular tarafından kullanılan en son tekniklerin analizini içeren [HP Wolf Security Threat Insights Raporunu](https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q4-2021/) yayınladı.

HP Wolf Security tehdit araştırma ekibi, kötü amaçlı yazılımları yaymak için Excel eklenti dosyalarını ele geçirerek, saldırganların hedeflere erişmesine yardımcı olan ve hem kurumları hem de bireyleri veri hırsızlığı ve yıkıcı fidye yazılımı saldırılarına maruz bırakan bir saldırı dalgası tespit etti. Sistemlere virüs bulaştırmak için kötü amaçlı Microsoft Excel eklentisi (.xll) dosyalarını kullanan saldırılarda geçen çeyreğe kıyasla altı kat büyük bir artış (**+%588**) yaşandı. Sadece bir tıklama gerektiren bu kötü amaçlı yazılımın özellikle tehlikeli olduğu tespit edilmiş bulunuyor. Ekip ayrıca yeraltı pazarlarında .xll dropper ve kötü amaçlı yazılım oluşturucu kitleri tanıtan reklamlar buldu. Tüm bunlar deneyimsiz saldırganların saldırı başlatmasını kolaylaştıran etkenler olarak öne çıkıyor.

Ayrıca, yeni bir QakBot spam saldırısı, güvenliği ihlal edilmiş e-posta hesaplarındaki e-posta zincirlerini ele geçirip postalara ekli bir kötü amaçlı Excel (.xlsb) dosyasıyla cevap yollayarak hedefleri kandırmak için Excel dosyalarını kullandı. QakBot, sistemlere girdikten sonra, algılanmamak için kendisini meşru Windows işlemlerine enjekte ediyor. Kötü amaçlı Excel (.xls) dosyaları, Ursnif bankacılık Truva’sını kötü amaçlı bir spam saldırısıyla İtalyanca konuşan kurumlara ve kamu sektörü kuruluşlarına yaymak için de kullanıldı ve saldırganlar [İtalyan kurye hizmeti BRT gibi davrandı](https://www.brt.it/alert-malware). Emotet kötü amaçlı yazılımlarını yayan yeni saldırılar artık JavaScript veya Word dosyaları yerine Excel'i de kullanıyor.

HP Wolf Security tehdit tespit ekibi tarafından yalıtılmış diğer önemli tehditler ise şunlar:

* **TA505 geri mi döndü?** HP, büyük kötü amaçlı yazılım spam saldırıları ve fidye yazılımlarını kullanarak virüslü sistemlere erişimden para kazanmasıyla bilinen finansal amaçlı bir tehdit grubu olan TA505 ile birçok taktik, teknik ve prosedür (TTP) paylaşan bir MirrorBlast e-posta kimlik avı saldırısı belirledi. Saldırı, FlawedGrace Uzaktan Erişim Truva Atı (RAT) ile kurumları hedef alıyor.
* **RedLine ile kurbanlara** bulaşan sahte oyun platformu: Ziyaretçileri RedLine infostealer'ı indirmeleri ve kimlik bilgilerini çalmaları için kandıran sahte bir Discord yükleyici web sitesi keşfedildi.
* **Nadir dosya tiplerini değiştirmek hala algılamanın önüne geçiyor:** Aggah tehdit grubu, satın alma emirleri olarak gizlenmiş kötü amaçlı PowerPoint eklenti (.ppa) dosyalarıyla Korece konuşan kurumları hedef aldı ve sistemlere uzaktan erişimli Truva atları bulaştırdı. Kötü amaçlı PowerPoint yazılımları olağandışı ve kötü amaçlı yazılımların %1'ini oluşturuyor.

HP Inc. Kıdemli Kötü Amaçlı Yazılım Analisti, HP Wolf Security tehdit araştırma ekibi üyesi Alex Holland “Kendilerini algılayacak araçlardan gizlenmek için yazılımların meşru özelliklerini kullanmak ve e-posta ağ geçitlerinin geçmesine izin verebilecek nadir dosya türlerinden faydalanmak saldırganlar için yaygın bir taktik. Güvenlik ekiplerinin sadece tespit etmekle yetinmemeleri, en son tehditlere ayak uydurmalarını ve savunmalarını buna göre güncellemeleri gerekiyor. Örneğin, gördüğümüz kötü amaçlı .xll görüntülerindeki spike'a dayanarak, ağ yöneticilerinin gelen .xll eklerini engelleyecek şekilde e-posta ağ geçitlerini yapılandırmasını, yalnızca güvenilir ortaklar tarafından imzalanmış eklentilere izin vermelerini veya Excel eklentilerini tamamen devre dışı bırakmalarını öneriyorum” diyor ve şöyle devam ediyor:

"Saldırganlar tespit edilmemek için sürekli yenilik yapıyor, bu nedenle kurumların savunmalarını tehdit ortamına ve kullanıcılarının iş ihtiyaçlarına göre planlamaları ve ayarlamaları hayati önem taşıyor. Tehdit aktörleri, e-posta zincirleri ele geçirme gibi tekniklere yatırım yaparak, kullanıcının dostu düşmandan ayırmasını her zamankinden daha zor hale getirdi.”

Bu bulgular, HP Wolf Security kullanan milyonlarca uç noktadan elde edilen verilere dayanıyor. HP Wolf Security, tüm enfeksiyon zincirini anlamak ve yakalamak için yalıtılmış mikro Sanal Makinelerde (mikro VM' ler) riskli görevler açarak kötü amaçlı yazılımları izliyor ve diğer güvenlik araçlarını geçen tehditleri azaltmaya yardımcı oluyor. Bu önlem, müşterilerin bildirilen bir ihlal olmadan 10 milyar e-posta eki açmasına, web sayfalarına ve indirmelere tıklamasına izin vermiş bulunuyor[[1]](#endnote-2). HP Wolf Security araştırmacıları ve mühendisleri, kötü amaçlı yazılımların davranışlarını daha iyi anlayarak uç nokta güvenlik korumasını ve genel sistem dayanıklılığını destekleyebiliyor.

Rapordaki diğer temel bulguları şunlar:

* Yalıtılmış e-posta kötü amaçlı yazılımlarının %13'ü en az bir e-posta ağ geçidi tarayıcısını atlamış.
* Tehditler, kurumlara virüs bulaştırma girişimlerinde 136 farklı dosya uzantısı kullanmış.
* Tespit edilen kötü amaçlı yazılımların %77'si e-posta yoluyla sisteme girerken, web indirmeleri %13'ünden sorumlu olmuş.
* Kötü amaçlı yazılım sokmak için kullanılan en yaygın ekler belgeler (%29), arşivler (%28), yürütülebilir dosyalar (%21), elektronik tablolar (%20) olmuş.
* En yaygın kimlik avı yemleri Yeni Yıl veya "Sipariş", "2021/2022", "Ödeme", "Satın Alma", "Talep" ve "Fatura" gibi ticari işlemlerle ilgili.

HP Inc. Kişisel Sistemler Küresel Güvenlik Başkanı Dr. Ian Pratt, "Bugün, düşük seviyeli tehdit aktörleri gizli saldırılar gerçekleştirebilir ve organize fidye yazılımı gruplarına erişim satabilir, bu da BT sistemlerini sakatlayan ve operasyonları durma noktasına getiren büyük ölçekli ihlallere yol açabiliyor” diyor ve ekliyor:

“Kurumlar, saldırı yüzeyini azaltmaya ve uzlaşma durumunda hızlı iyileşme sağlamaya odaklanmalı. Bu, Sıfır Güven ilkelerini takip etmek ve donanım düzeyinden itibaren güçlü kimlik yönetimi, en az ayrıcalık ve yalıtım uygulamak anlamına gelir. Örneğin, mikro sanallaştırma kullanarak e-posta, tarayıcı veya indirme gibi yaygın saldırı vektörlerini izole ederek, içinde gizlenen olası kötü amaçlı yazılımlar veya istismarlar kontrol altına alınır ve böylece zararsız hale getirilirler.”

**İlgili Kişiler**Ceren Moral Aru – 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)

**Veriler hakkında**

Bu veriler Ekim-Aralık 2021 tarihleri arasında HP Wolf Security müşteri sanal makinelerinde toplanmıştır**.**

-

**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>

**HP Wolf Security hakkında**

Dünyanın en güvenli bilgisayarlarının ve yazıcılarının üreticisi olan HP Wolf Security, yeni bir uç nokta güvenliği türüdür. HP'nin donanımla zorlanan güvenlik ve uç nokta odaklı güvenlik hizmetleri portföyü, kuruluşların bilgisayarları, yazıcıları ve insanları siber avcılardan korumasına yardımcı olmak için tasarlanmıştır. HP Wolf Security, donanım düzeyinde başlayan ve yazılım ve hizmetlere yayılan kapsamlı uç nokta koruması ve esnekliği sağlar.[[2]](#endnote-3) [[3]](#endnote-4) [[4]](#endnote-5)

1. Müşteri tarafından bildirilen tespitlerin ve yüklü tabanın HP dahili analizine dayanan varsayımlar. [↑](#endnote-ref-2)
2. Windows ve 8th Gen ve daha yüksek Intel® işlemcilere veya AMD Ryzen™ 4000 işlemcilere ve daha yükseğine, ayrıca Intel® 10th Gen ve daha yüksek işlemcili HP ProDesk 600 G6; ve AMD Ryzen™ 4000 veya Intel® 11th Gen işlemcili HP ProBook 600 ve üstüne sahip HP Elite bilgisayarlardaki satıcılar arasında ek ücret ödemeden HP'nin benzersiz ve kapsamlı güvenlik özelliklerine dayanmaktadır; [↑](#endnote-ref-3)
3. HP'nin en gelişmiş gömülü güvenlik özellikleri, HP FutureSmart ürün yazılımı 4.5 veya üzeri HP Enterprise ve HP Managed cihazlarda kullanılabilir. Tespitler 2021'de yayınlanan rekabetçi sınıf yazıcıların özelliklerinin HP incelemesini esas alır. Yalnızca HP, cihaz siber dayanıklılığı için NIST SP 800-193 yönergeleriyle uyumlu olarak, kendi kendini iyileştiren yeniden başlatma ile saldırıları otomatik olarak algılamak, durdurmak ve kurtarmak için güvenlik özelliklerinin bir birleşimini sunar. Uyumlu ürünlerin listesi için şu adresi ziyaret ediniz: [hp.com/go/Yazıcılar Bu Koruma](http://www.hp.com/go/PrintersThatProtect). Daha fazla bilgi için şu adresi ziyaret edin: [hp.com/go/PrinterSecurityClaims](http://www.hp.com/go/printersecurityclaims) [↑](#endnote-ref-4)
4. HP Security artık HP Wolf Security'dir. Güvenlik özellikleri platforma göre değişir, ayrıntılar için lütfen ürün veri sayfasına bakınız. [↑](#endnote-ref-5)