|  |
| --- |
| Basın Bülteni**HP’nin Siber Güvenlik Tehdit Raporu’na göre tespit edilen kötü amaçlı yazılımların yüzde 75'i e-posta yoluyla gönderiliyor**HP Wolf Security tehdit araştırma ekibinin bulgularına göre, siber suçlar gelişirken para kazanma ve bilgisayar korsanlığı araçlarında patlama yaşanıyor. Bununla birlikte son kullanıcıların hala eski yöntemlere karşı savunmasız olduğu görülüyor. |

HP (NYSE: HPQ), siber güvenlik saldırılarının ve güvenlik açıklarının analiz edildiği en güncel küresel [Tehdit Öngörüleri Raporu](https://threatresearch.ext.hp.com/wp-content/uploads/2021/07/HP_Wolf_Security_Threat_Insights_Report_H1_2021.pdf)’nu yayınladı. Araştırma, 2020 yılının ikinci yarısından 2021 yılının ilk yarısına kadar dosya paylaşım web sitelerinden indirilen siber saldırı araçlarının kullanımında yüzde 65'lik artış olduğunu gösteriyor.

Araştırmacılar geniş sirkülasyona sahip siber saldırı araçlarının birçok özelliğe sahip olduğunu aktarıyor. Örneğin web sitelerine karşı kimlik bilgisi doldurma saldırıları gerçekleştirmek için optik karakter tanıma (OCR) gibi bilgisayarla görme tekniklerini kullanarak CAPTCHA zorluklarını çözebiliyor.

**HP Kişisel Sistemler Güvenlik Küresel Başkanı Dr. Ian Pratt**, konuyla ilgili şunları söyledi:

“Siber saldırı araçlarının ve yeraltı forumlarının yaygınlaşması, daha önce düşük seviyeli aktörlerin kurumsal güvenlik için ciddi riskler oluşturmasına izin veriyor. Aynı zamanda kullanıcılar basit kimlik avı saldırılarının kurbanı olmaya devam ediyor. BT departmanlarını gelecekteki tehditleri gerçekleşmeden engelleyecek şekilde donatan güvenlik çözümleri, şirketlerin korumasını ve esnekliğini en üst düzeye çıkarmanın anahtarı olarak kilit role sahip.”

HP Wolf Security’nin tespit ettiği önemli tehditler arasında aşağıdakiler yer alıyor:

* **Siber suçlular birlikte çalışarak daha büyük saldırılara kapı açıyor:** Dridex ile bağlantılı taraflar, fidye yazılımını dağıtabilmek için ele geçirilen şirketlere erişimi diğer tehdit aktörlerine satıyor. 2021 yılının ilk çeyreğinde Emotet etkinliğindeki düşüş, Dridex'in HP Wolf Security tarafından tespit edilen en gelişmiş kötü amaçlı yazılım ailesi haline gelmesine yol açtı.
* **Bilgi hırsızları daha büyük sonuçlara neden olan kötü amaçlı yazılımlar sunuyor:** Geçmişte kripto para cüzdanlarından ve web tarayıcılarından kimlik bilgilerini almak için bilgi hırsızı olarak kullanılan CryptBot kötü amaçlı yazılımı, organize suç grupları tarafından çalıştırılan bir bankacılık truva atı olan DanaBot'u sızdırmak için de kullanılıyor.
* **Şirket yöneticilerini hedefleyen VBS indirme çalışmaları:** Çok aşamalı bir Visual Basic Komut Dosyası (VBS) çalışması, hedeflediği yöneticinin adını taşıyan kötü amaçlı ZIP eklerini paylaşıyor. Daha sonra cihazlarda kalıcı olmak ve kötü amaçlı yazılım dağıtmak için meşru SysAdmin araçlarını kullanmadan önce gizli bir VBS indiricisi kuruyor.
* **Uygulama olarak başlayan yazılımlar şirketlere sızıyor:** Yedi ülkedeki (Şili, Japonya, İngiltere, Pakistan, ABD, İtalya ve Filipinler) nakliyat, denizcilik, lojistik ve ilgili şirketleri hedef alan ve dağıtmak için Microsoft Office’in bir güvenlik açığından yararlanan ve özgeçmiş gibi görünen (résumé-themed) kötü niyetli spam çalışmalarıyla mevcut Remcos RAT ve virüslü bilgisayarlara arka kapı erişimi elde ediliyor.

**HP Kıdemli Kötü Amaçlı Yazılım Analisti Alex Holland** ise “Siber suç ekosisteminde küçük siber suçluların, organize suç içindeki daha büyük oyuncularla bağlantı kurma ve savunmaları atlayıp sistemleri ihlal edebilen gelişmiş araçları indirme imkanı artıyor. Bu yüzden ekosistem gelişmeye ve dönüşmeye devam ediyor. Siber saldırganların tekniklerini daha fazla para kazanacak şekilde değiştirdiğini ve şirketlere karşı daha karmaşık saldırılar başlatabilmeleri için organize suç gruplarına erişim sattığını görüyoruz. CryptBot gibi kötü amaçlı yazılım türleri, önceden bilgisayarlarını kripto para cüzdanlarını depolamak için kullanan kullanıcılar için bir tehlike oluşturuyordu. Ancak şimdi şirketler için de bir tehdit haline geldi. Bilgi hırsızlarının siber saldırı araçlarına erişimlerinden para kazanmak için fidye yazılımlarını tercih etme eğiliminde olan organize suç grupları tarafından çalıştırılan kötü amaçlı yazılımları dağıttığını görüyoruz” dedi.

Rapordaki diğer önemli bulgular aşağıda yer alıyor:

* Tespit edilen kötü amaçlı yazılımların yüzde 75'i e-posta yoluyla gönderilirken, kalan yüzde 25'i de web sitelerinden indirildi. Web tarayıcıları kullanılarak indirilen tehditler, dolaylı da olsa siber saldırı araçlarını ve kripto para madenciliği yazılımını indiren kullanıcılar nedeniyle yüzde 24 arttı.
* En yaygın e-posta oltalama denemeleri yüzde 49 ile faturalar ve ticari işlemler üzerinden gerçekleştirilirken, yüzde 15'i de ele geçirilen e-posta ileti dizilerine verilen yanıtlar ile yapıldı. COVID-19'dan bahseden oltalama tuzakları, 2020'nin ikinci yarısından 2021'in ilk yarısına yüzde 77 düşerek yüzde 1'den daha azını oluşturdu.
* En yaygın kötü amaçlı ek türü arşiv dosyaları (yüzde 29), elektronik tablolar (yüzde 23), belgeler (yüzde 19) ve çalıştırılabilir dosyalar (yüzde 19) oldu. JAR (Java Arşiv dosyaları) gibi olağandışı arşiv dosyası türleri, algılama ve tarama araçlarından kaçınmak ve yeraltı pazarlarında kolayca elde edilebilen kötü amaçlı yazılımları yüklemek için kullanılıyor.
* Rapor, yakalanan kötü amaçlı yazılımların yüzde 34'ünün önceden bilinmediğini ve bu tür kötü amaçlı yazılımların 2020'nin ikinci yarısına kıyasla yüzde 4 düştüğünü buldu.
* Microsoft Office veya Microsoft WordPad'den yararlanmak ve dosyasız saldırılar gerçekleştirmek için yaygın olarak kullanılan güvenlik açığı CVE-2017-11882'den faydalanan kötü amaçlı yazılımlarda yüzde 24'lük bir artış gözlemleniyor.

**Veri hakkında**

Bu veriler, Ocak - Haziran 2021 arasında HP Wolf Security müşterilerinin sanal makinelerinde toplandı.

**İlgili Kişiler**Ceren Moral Aru – Bordo PR
0533 921 43 53
cerenm@bordopr.com
Beril Pelesen – Bordo PR
0537 220 49 39
berilp@bordopr.com

## **HP hakkında**

HP  Inc. hayatı herkes için her yerde iyileştiren bir teknoloji yaratıyor. Kişisel sistemler, yazıcılar ve 3 boyutlu yazıcı çözümlerinden oluşan ürün ve servis portfolyomuz insanı şaşırtan tecrübeler yaratıyor. HP  hakkında daha fazla bilgiye [http://www.hp.com](http://www.hp.com/) sitesinden ulaşabilirsiniz.