Bilgi Notu **16 Temmuz 2019**

Türkiye'ye Özel Siber Tehdit Türkiye'deki Kurumların Başına Bela Oldu

Türkiye'deki kurumları hedefleyen 'Oto Gönderici' adlı tehdidi bir süredir yakın takibe alan Sophos güvenlik uzmanları, bulgularını detaylı bir rapor eşliğinde paylaştı. Geçtiğimiz sonbahar aylarından beri yoğun spam kampanyalarıyla Türkiye'deki şirketleri baskı altında tutan bu tehdit, kullandığı alışılmadık yöntem sayesinde bazı uç nokta güvenlik çözümlerinin gözünden kaçmayı başarıyor.

Sophos güvenlik uzmanları, geçtiğimiz sonbahardan beri istenmeyen e-posta mesajları aracılığıyla yayılan ve özellikle Türkiye'deki kurumları ağına düşürmeyi hedefleyen "Oto Gönderici" adlı tehdide dair **detaylı bir rapor** yayınladı. Eğitimden sağlığa, kamudan enerjiye tüm sektörleri tehdit eden Oto Gönderici, kullandığı Excel Formula Injection adlı alışılmadık saldırı tekniği sayesinde bazı uç nokta güvenlik ürünlerinin gözünden kaçabiliyor.

Bir süredir Türkiye'deki kurumları etkisi altına alan bu tehdit, Türkçe hazırlanmış spam mesajları aracılığıyla yayılan dosya eklerinin açılmasıyla bulaşıyor. Nadir olarak uluslararası alanda görülen tehdidin Türkiye dışında da Türkçe dilini kullanması ve diğer bazı ipuçları, tehdidin Türkiye'de doğmuş olabileceğine işaret ediyor. Gönderilen mesajların benzer ifadelere sahip olması ve gönderim için seçilen adreslerin genelde info@ posta kutularına yönlendirilmesi, saldırıların özel bir kurum veya sektör yerine genel dağıtıma odaklandığını gösteriyor.

Otomasyon Sistemi Kurmuşlar, Vazgeçmeye Niyetleri Yok

Oto Gönderici, istenmeyen e-posta eklerinde yer alan dosyaların açılmasıyla sisteme bulaşıyor. Zaman içinde farklı yöntemler deneyen tehdidin favorisi geçtiğimiz yıl keşfedilen Excel Formula Injection adlı teknik. Excel Formula Injection, metin tabanlı CSV tabloların içine ustaca gömülen kodlar yardımıyla PowerShell'i aktif hale getirerek saldırganlara ait internet sunucularından Truva Atı yazılımının indirilmesini ve kurulmasını sağlıyor. Microsoft Excel'in söz konusu dosyanın kod çalıştırmaya hazırlandığına dair yaptığı uyarılara rağmen kullanıcı onay verip devam eder ve saldırı başarılı olursa, Adwind veya FareIt gibi Truva Atı yazılımlarının yüklenmesiyle sistemler yetkisiz erişime açık hale getiriliyor.

Oto Gönderici, diğer özelleşmiş tehditlere kıyasla daha basit bir yapıya sahip olsa da gücünü saldırganların inatçılığından alıyor. Sophos'a sürekli gelen yeni örnekler saldırganların vazgeçmeye niyetli olmadığını, gönderimlerin ısrarla devam ettiğini, hatta bu iş için otomasyon sistemi kurulduğunu gösteriyor.

SophosLabs'ın Oto Gönderici hakkındaki detaylı analizini https://news.sophos.com/en-us/2019/07/11/oto-gonderici-excel-formula-injections-target-turkish-victims/ adresinde bulabilirsiniz.