ATM/POS Güvenliği Hizmetleri

ATM'ler ve POS cihazları artık yalnızca ATM hırsızlığı veya kart kopyalama gibi fiziksel saldırılara açık değildir. Bankaların ve ATM/POS tedarikçilerinin aldığı önlemler geliştikçe, bu cihazlara karşı düzenlenen saldırılar da hızla daha karmaşık hale gelmektedir. Bilgisayar korsanları, ATM/POS altyapı mimarilerindeki ve uygulamalarındaki güvenlik açıklarından yararlanır; ATM/POS cihazlarına özel olarak kötü amaçlı yazılımlar geliştirirler. Kaspersky Lab ATM/POS Güvenlik Değerlendirmesi hizmetleri, ATM/POS cihazlarındaki güvenlik kusurlarını fark etmenizi ve sistemlerinizin ele geçirilme riskini azaltmanızı sağlar.

Bunun için kapsamlı koruma sağlayan tek bir çözüm yoktur. Bir işletme yöneticisi olarak, kurumunuzu günümüzdeki tehditlere karşı korumak ve gelecekte karşılaşılabilecek tehlikeleri öngörmek sizin görevinizdir. Bunun için yalnızca bilinen tehditlere karşı akıllı işlemsel koruma yeterli değildir; üst düzey stratejik güvenlik istihbaratına da ihtiyaç duyulur. Çok az şirket bu düzeyde bir istihbaratı kurum içinde geliştirebilecek kaynaklara sahiptir.

Kasperksy Lab Güvenlik Değerlendirme Hizmetleri: Bilgi ve deneyimleri ile güvenlik istihbaratında dünya lideri olmamızı sağlayan, birçoğu kendi alanında, dünya çapında tanınmış otoriteler olan kurum içi uzmanlarımızın sunduğu hizmetler.

ATM/POS
Güvenlik Değerlendirmesi

Saldırganlar tarafından şu amaçlarla kullanılabilecek güvenlik açıklarını tespit etmek için tasarlanmış kapsamlı ATM ve POS cihazı analizi:

- İzinsiz para çekme
- İzinsiz işlem yapma
- Müşterilerinizin ödeme kartı bilgilerini ele geçirme
- Hizmeti engelleme saldırısı başlatma

Bunu neden yapmalısınız?

Kaspersky Lab tarafından sağlanan ATM/POS Güvenlik Değerlendirmesi satıcılara ve finansal kuruluşlara şu konularda yardımcı olur:

- ATM/POS cihazlarındaki güvenlik açıklarını anlayabilir ve ilgili güvenlik süreçlerinizi buna göre geliştirebilirsiniz.
- Saldırganların yararlanabileceği güvenlik açıklarını proaktif bir şekilde tespit edip düzelterek saldırının neden olabileceği finansal ve işlemsel zararları ve itibar kayıplarını önleyebilirsiniz.
- PCI DSS (Ödeme Kartı Sektörü Veri Güvenliği Standartları) gibi güvenlik değerlendirmesi uygulamayı zorunlu kılan resmi, sektörel ve kurumsal standartlara uyum sağlarsınız.

Dolandırıcılar içeri sızarsa ne olur?

Her ATM makinesi, her birinde 3000'e kadar banknot bulunan 4 kasetten oluşur. En kötü durumda, suçlular 255.000 USD'ye kadar para ele geçirebilir. Mayıs 2016'da gerçekleşen ATM dolandırıcılığı, suçluların, eylemlerini birkaç saatlik bir zaman dilimi içerisinde 1400 ATM makinesine erişebilecek şekilde koordine edebildiklerini gösterdi. Haziran 2016'da, Tayvan'da birçok ATM'ye kötü amaçlı yazılım yüklenmesiyle meydana gelen olay, suçluların yirmi ATM'den 2 milyon USD çekmesine yol açtı. Suçlular ATM'lere saldırmaya hazır. Mağdur olmayın.

Biz kimiz?

Proje ekibi üyeleri, alan hakkında kapsamlı bilgiye sahip, becerilerini sürekli geliştiren, güvenlik uygulamalarında son derece deneyimli uzmanlardır. Düzenli olarak ATM/POS satıcılarına güvenlik danışmanlığı sağlar ve ATM/POS güvenlik araştırmalarımızın sonuçlarını Black Hat, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack, HITB GSEC, DefCamp, ATMIA events ve Chaos Communication Congress gibi bir çok önde gelen bilgi güvenliği konferansında sunarlar.

Uzmanlarımızı takip etmek için: www.securelist.com

Yardım için bize ulaşın: 1337@kaspersky.com

Neyi test ediyoruz?

Hizmet; yazılım bileşenlerinin, donanım cihazlarının ve ağ bağlantılarının değerlendirilmesi dahil kapsamlı ATM/POS analizini içerir. Hizmet, tek bir ATM/POS cihazı veya birçok cihazın yer aldığı bir ağ için gerçekleştirilebilir. Değerlendirme için kurumunuzda en çok kullanılan ATM/POS cihazı türünü veya tipik yapılandırmaları konusunda en kritik olan cihazları (örneğin önceden bir saldırıya maruz kalmış cihazlar) seçmenizi öneririz.

Bunu nasıl yapıyoruz?

Analiz sırasında uzmanlarımız yalnızca yapılandırma hatalarını ve eski yazılım sürümlerindeki güvenlik açıklarını arayıp tespit etmekle kalmaz, aynı zamanda ATM/POS cihazlarınızın gerçekleştirdiği işlemlerin arkasındaki mantığı derinlemesine analiz ederek bileşen seviyesinde yeni (0 gün) açıklarını tanımlamaya yönelik güvenlik araştırması yaparlar. Bir saldırganın kullanabileceği güvenlik açıkları (örneğin izinsiz para çekmeye yol açabilecek açıklar) tespit ettiğimiz takdirde, uzmanlarımız özel olarak üretilmiş otomasyon araçlarını ve cihazlarını kullanarak olası saldırı senaryolarını gösterebilir.

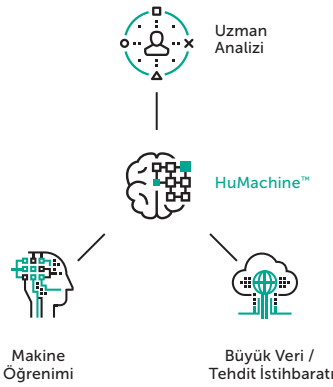
Bir ATM/POS Güvenlik Değerlendirmesi, savunma stratejilerinizin etkililiğini değerlendirmek için gerçek bir korsanın saldırı yöntemini taklit etse de tamamen güvenlidir ve sistemlerinize müdahale etmez.

Finans Sektörüne Yönelik Tehditler

Finansal işletmelerin doğası gereği bankalar, borsalar ve diğer finansal kuruluşlar siber suçluların daimi ilgi alanı içerisindedir. Bu nedenle finans sektörü mali kayıpları ve itibar kaybını önlemek için siber güvenlik alanında hep çağının ötesinde durmalıdır. Kaspersky Lab, güvenlik işlemlerini geliştirmek ve ileri düzeydeki tehditlere karşı proaktif bir yaklaşım benimsemek isteyen finansal kuruluşlara bir dizi proaktif tehdit istihbaratı hizmeti sunar:

- Güvenlik Değerlendirme Hizmetleri (Sızma Testi, Uygulama Güvenliği Değerlendirmesi, ATM ve POS Güvenliği Değerlendirmesi)
- Tehdit İstihbaratı Raporları (APT İstihbaratı Raporları, Müşteriye Yönelik Tehdit İstihbaratı Raporları)
- Siber Saldırı Hazırlığı Testi
- Botnet Tehdit Takibi
- Tehdit Veri Akışları
- Kötü Amaçlı Yazılım Analizi ve Adli Bilişim
- Eğitim: Tehdit Analizi, Adli Bilişim ve İnceleme

Daha fazla bilgi için: www.kaspersky.com.tr/enterprise



Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenlik Haberleri: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr