Kaspersky® Embedded Systems Security

ATM ve POS Güvenlik Kılavuzu

Gömülü cihazlar için standart güvenlik düzenlemeleri, genellikle yalnızca virüsten koruma tabanlı güvenlik ve sistem güçlendirmesini kapsar, bu da yeterli değildir. Tamamen virüsten koruma tabanlı bir yaklaşım, mevcut gömülü sistem tehditleri karşısında yeterince etkili değildir. Yakın zamanda gerçekleştirilen saldırılarda da bu durum fazlasıyla görülmüştür. Artık Cihaz Kontrolü ve Varsayılan Olarak Reddet gibi başarısını kanıtlamış teknolojilerin yanı sıra gerektiğinde kritik sistemlere ek Virüsten Koruma modülü uygulanmalıdır.

Gömülü sistemler, kendilerine özgü güvenlik sorunlarına sahiptir. Genellikle coğrafi olarak farklı yerlere dağıtılmış şekildedir. Bu sistemlerin yönetilmesi zor olabilir ve sistemler nadiren güncellenir. Gerçek para ve kredi kartı kimlik bilgileriyle çalışan ATM'ler ve Satış Noktası cihazları, siber suçluların tercih ettiği hedeflerdir. Bu nedenle en yüksek düzeyde odaklı ve akıllı koruma gerektirir.

Sorunlar

Eski yazılım çok yaygın bir sorundur ve bu sorundan yalnızca tüketici işletim sistemleri etkilenmez. Hâlâ faaliyet göstermekte olan bazı uzay uydularının bile çok eski donanımlar ve yazılımlar kullandığı bilinen bir gerçektir. Endüstriyel kontrol sistemleri de çok eski işletim sistemleri ve uzun yenileme döngüsü sorunlarıyla karşı karşıyadır. Aynı şey yalnızca uç noktalar için değil, bankacılık sistemleri için de geçerlidir. Dahili otomatik bankacılık sistemleri genellikle yıllarca güncellenmez. ATM'lerde ise küçük bankaların %80'i, yeni sürümler çıktıkça yazılımları güncellemek yerine bir sonraki döngü sonuna (5-10 yıl, hatta daha uzun sürebilir) kadar bekledikten sonra yeni yazılımların yüklü olduğu yeni makineler satın alır.

Windows XP aileleri, ATM ve POS cihazları için hâlâ en popüler işletim sistemleridir. Bu işletim sistemine verilen desteğin sona ermesi, çok sayıda işletme ve devlet kurumunu etkilemiştir. Dünya genelinde çok sayıda ATM'nin Windows XP Professional for Embedded Systems sürümünü kullandığı bankacılık ve perakende sektörü de bu değişimden en çok etkilenenler arasındadır. Aslında bu sistem, Windows XP'nin tüketici sürümleriyle birlikte 2014 yılının Nisan ayında desteklenmemeye başlamıştır.

Ancak ATM ve POS sistemlerinin değiştirilmesi, genel olarak uzun, pahalı ve can sıkıcı bir süreçtir. Ayrıca yazılımın değiştirilmesi genellikle, çalışmaya devam etmesine rağmen teknik olarak eski donanımların değiştirilmesini gerektirir.

Tehdit Ortamı

Bankanın fiziksel güvenlik çevresi dışında çalışan ve nakit para içeren ATM'ler ve doğrulanmış kişisel verilerin yanı sıra kredi kartı bilgilerine sahip olan POS sistemleri, kaçınılmaz olarak siber suçluların kara listesine girer.

Skimer kötü amaçlı yazılımının faaliyetleriyle 2009 yılında ATM'lere yapılan ilk ciddi saldırıdan itibaren her geçen yıl saldırıların sayısı ve kalitesi önemli ölçüde artmıştır. 2015 yılında Ploutus, Tyupkin, Carbanak, CardStealer, vSkimmer, Chewbacca, POSeydon ve FindPOS gibi kötü amaçlı yazılımlarla ATM ve POS sistemlerine yapılan saldırılar yeni bir rekor kırmıştır.

Geleneksel virüsten koruma yazılımları, tüm bu tehditlere karşı tam koruma sağlayamaz. ATM ve POS sistemlerinin sınırlamaları (zayıf kanallar, düşük teknoloji ürünü donanım ve eski yazılımlar) ise virüsten koruma yazılımlarının kurulumunu ve dağıtımını zor ve bazen imkansız hale getirir. Dolayısıyla bu virüsler, her gün büyük finans kuruluşlarının ve perakendecilerin ATM ve POS sistemlerine sızma konusunda başarılarını sürdürmektedir.

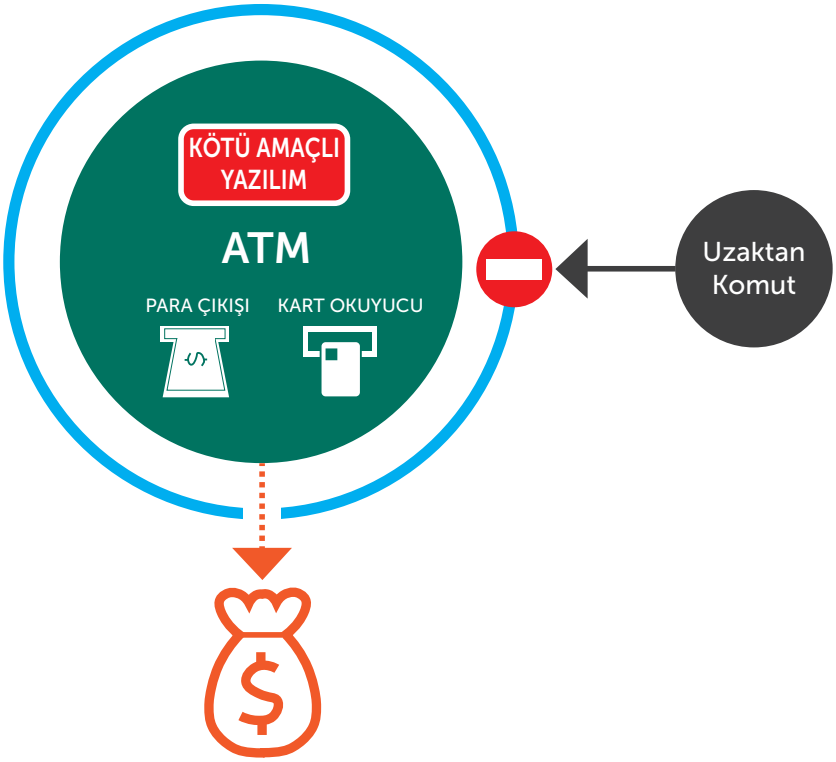
Ayrıca en yeni ve en güçlü sistemler ve donanımlarla desteklenen profesyonel geliştiriciler, giderek artan sayıda hedefli ATM ve POS kötü amaçlı yazılımları üretmektedir.

ATM Saldırı Şeması

Coğrafi olarak dağılmış ATM uç noktaları, hedefli bir saldırının parçası olarak kötü amaçlı yazılımın sisteme sızdırılması için ideal giriş noktalarıdır. Özellikle USB erişim bağlantı noktalarının ve klavyelerin, ATM'nin arkasındaki sistem servis kabinlerinde kolayca ulaşabilir bir yere konumlandırılmış olması ve yalnızca basit bir kilitle korunuyor olması, ATM'leri daha cazip hale getirir.

Hatta kilit bile siber suçlular için bir sorun oluşturmayabilir. Yerel servis mühendislerinin kapıyı açma zahmetinden kurtulmak için ATM servis kabininden çıkan yarı kalıcı bir USB veya LAN/modem kablosu kullanması oldukça sıradandır. Ancak servis mühendisleri, bu USB bağlantı noktalarını ve CD/DVD sürücülerini makine bakımında sıklıkla kullandığı için bunları devre dışı bırakarak güvenliği artırmak pratik bir çözüm değildir.

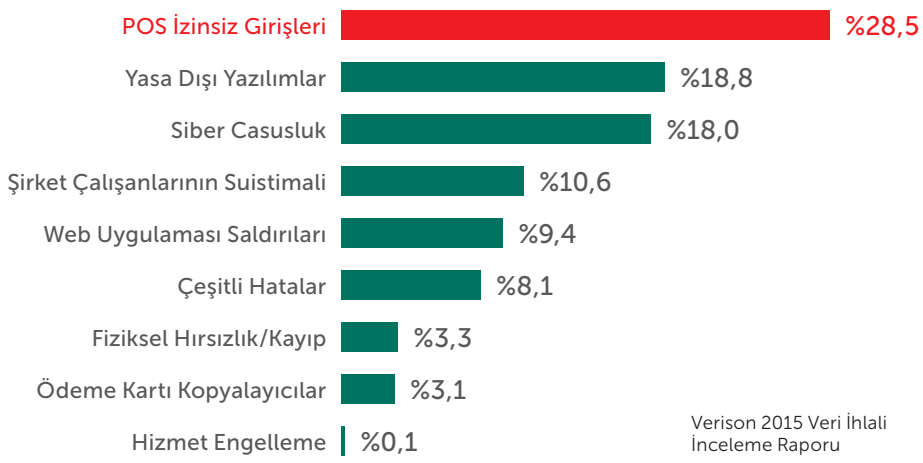
Kötü amaçlı yazılım, bir makine üzerinden ATM sistemine girdikten sonra bir süre gizlenip sistemin normal bir şekilde çalışmasına izin verebilir. Bu sürede saldırganlar daha fazla bilgi toplar ve hazırlık yapar. Daha sonra zamanı geldiğinde sistem mantığındaki değişiklikleri tetiklemek için belirli bir kart veya PIN kullanılabilir. Sistem mantığındaki bu değişiklik nedeniyle yazılımın bulaştığı tüm ATM'ler, talep üzerine içindeki paraları suçlulara verir.



Basit bir ATM saldırısı, nakit para almanın hızlı ve kolay bir yoludur. Ancak ATM virüsleri, çok daha geniş bir saldırı senaryosunun bir parçası da olabilir. 2015 yılında Carbanak gibi Gelişmiş Sürekli Tehdit Saldırılarının, dünya genelinde 1 Milyar USD'den daha fazla finansal kayba neden olabileceğini gördük.

POS Tabanlı Tehditler

BT Güvenlik Olaylarının Sıklığı
Onaylanan Veri İhlallerinin Sınıflandırılması



Verison 2015 Veri İhlali İnceleme Raporu

Varsayılan Olarak Reddet

Geleneksel antivirüs çözümlerinin çoğu, endüstrinin günümüzde karşı karşıya olduğu bu tür gelişmiş ve hedefli kötü amaçlı yazılım tehditlerine karşı tam koruma sağlayamaz. Varsayılan Olarak Reddet işlevi farklı ve daha temel bir yaklaşım gerektirir. Yazılım koruması dışındaki hiçbir yürütülebilir dosya, sürücü ve kitaplık, Güvenlik Yöneticisi'nden merkezi onay almadan herhangi bir ATM veya POS uç noktasında çalışamaz.

Cihaz Kontrolü

Kaspersky Lab Cihaz Kontrolü, sistem donanımına fiziksel olarak bağlanmayı deneyen USB depolama cihazlarını kontrol etme özelliği sunar. Böylece ATM veya POS ünitesine yetkisiz bir cihaz tarafından erişimi engeller. Bu sayede siber suçluların kötü amaçlı yazılım saldırılarında ilk adım olarak kullandığı savunmasız sistem giriş noktaları engellenir.

Windows XP – Windows 10 Desteği

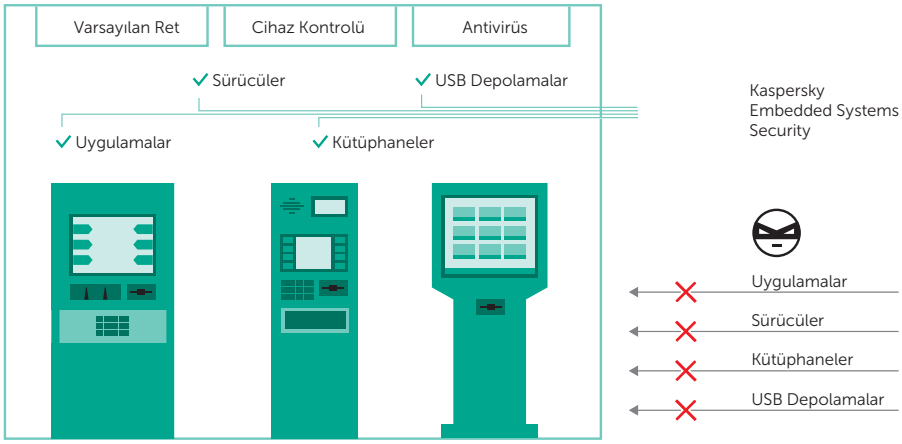
12 yıl sonra, 12 Ocak 2016'da Windows XP Embedded desteği ve 12 Nisan 2016'da Windows Embedded for Point of Service desteği sona ermiştir. Windows XP işletim sistemi için artık güvenlik güncellemesi veya teknik destek hizmeti verilmemektedir. Kaspersky Embedded Systems Security, Windows XP ailesi için %100 destek sağlar.

Gömülü Sistem Donanımları İçin Tasarlanmıştır

Kaspersky Embedded Systems Security, ATM ve POS donanımlarının birçoğunda kullanılan alt uç sistemlerinin tam etkinlik göstermesi için tasarlanmıştır. Windows XP ailesi için gereksinimler 256 MB RAM'den başlar ve sistem sabit sürücüsünde yaklaşık 50 MB'lik boş alan yeterlidir. "İstek üzerine" modunda çalışırken, ayrı olarak yüklenen virüsten koruma modülü, yalnızca manuel veya zamanlanmış taramalar sırasında donanım kaynaklarını kullanmak üzere tasarlanmıştır.

Virüsten Koruma Yazılımı ve Kaspersky Security Network

PCI DSS gereklilikleri, kredi veya banka kartlarıyla çalışan tüm sistemlerde virüsten koruma yazılımının yüklü olmasını ve düzenli olarak güncellenmesini gerektirir. Kaspersky Embedded Systems Security, gerektiğinde düzenli otomatik veya manuel kötü amaçlı yazılım imza güncellemeleriyle birlikte virüslere karşı etkili koruma sağlar. ATM ve POS sistemlerinde bulunan tüm kötü amaçlı yazılımların yarısından fazlası sıfır gün güvenlik açıkları aracılığıyla sisteme girdiği için Kaspersky Lab, Kaspersky Security Network bilgi veritabanı biçiminde akıllı güvenlik uygulamayı önerir. Bu sayede açıklardan yararlanan yazılım tabanlı güvenlik risklerini önleme ve azaltma sağlanır ve tepki süresi en aza indirilir.



Satış Noktası sistemleri, bir ara yazılıma dayanır. Bu ara yazılım, Satış Noktası sistemlerine özgü bir güvenlik açığı oluşturur. Bu ara yazılımlar, genellikle küçük üçüncü taraf satıcıları veya şirket içi ekipler tarafından geliştirilir. Tasarım açısından işlevsellik, güvenlikten önce gelebilir. Ayrıca tıpkı ATM'lerde olduğu gibi bağlantı noktalarına ve CD/DVD sürücülerine kolay erişim sağlanması, güvenlik zayıflığından çok kullanışlı bir özellik gibi görünebilir.

POS sistemlerinin çoğu, kredi/banka kartlarıyla çalıştığı için ATM'ler gibi PCI/DSS düzenlemesine tabidir. İstisnasız tüm POS sistemleri kişisel müşteri verileriyle çalışır. Bu verilerin korunması, POS sistemleri sahibinin sorumluluğundadır. Ayrıca tüm POS sistemleri bir intranete bağlı olduğu için Hedefli Saldırılar'da kullanışlı bir giriş noktası haline gelirler.

Kaspersky Embedded Systems Security

Kaspersky Lab, ATM ve POS sistemleri kullanan kuruluşlar ve bu kuruluşların içinde bulunduğu tehdit ortamı için özel bir güvenlik çözümü geliştirmiştir. Bu çözüm, ilgili sistemlerin işlevselliğinin ve işletim sistemin yanı sıra kanal ve donanım gereksinimlerini de yansıtır. Ayrıca Windows XP ailesini tam olarak destekler.

Kaspersky Embedded Systems Security, gömülü sistemlerin yapısında bulunan güvenlik risklerini azaltır. Bu çözüm, özellikle ATM ve POS sistemleri için geliştirilmiştir ve bu sistemlerin mimarisine özgü saldırı alanlarını korurken aynı zamanda ilgili donanıma ve verimlilik etkenlerine uyum sağlar. Tek bir sezgisel konsol, uç noktalarınızın, kritik sistemlerinizin ve tüm BT altyapınızın etkili ve çok katmanlı güvenliğini yönetmek için ihtiyacınız olan kontrolü ve görünürlüğü sağlar.

Cihaz Kontrolü işleviyle güçlendirilen Uygulamalar, Sürücüler ve Kitaplıklar için "Varsayılan Olarak Yasakla" özelliğini uygulamak, hâlâ kullanılmakta olan teknik açıdan "eski" sistemlerin güvenliğini sağlayabilecek tek yaklaşımdır.

Kaspersky Embedded Systems Security, "Yalnızca Varsayılan Olarak Yasakla" çalışma modu özelliğinin yanı sıra 256 mb RAM ve 50 mb boş sabit disk sürücü alanından başyan sistem gereklilikleri sağlar. Bu nedenle alt uç donanımlarda çalışan Windows XP tabanlı sistemler için idealdir. İsteğe bağlı tarama, Kaspersky Security Network tarafından desteklenen opsiyonel bir Virüsten Koruma modülü aracılığıyla sağlanır ve bu modül, gerektiğinde Düzeltme Eki Yönetimi özellikleri sağlar.

Yani bu tek çözüm şu üç temel ihtiyacı karşılar:

- "Yönetmesi zor" sistemlerin etkili bir şekilde korunması
- PCI DSS gereklilikleri 5.1, 5.1.1, 5.2, 5.3 ve 6.2 ile uyum
- Eski sistemler ve donanım değişimi için esnek zaman çizelgesi sağlama.

PCI DSS Uyumluluğu

Kaspersky Security for Embedded Systems işlevleri, PCI DSS v3.2 alt maddelerinde belirtilen tüm güvenlik standartlarını karşılar ve aşar:

1.4: Ağ dışındayken internete bağlanan ve aynı zamanda CDE'ye (Kart Verileri Ortamı) erişim için kullanılan taşınabilir bilgi işlem cihazlarına kişisel güvenlik duvarı yazılımı yükleyin.

2.4a: PCI DSS kapsamındaki sistem bileşenlerinin bir envanterini tutun.

5.1: Virüsten koruma yazılımını, kötü amaçlı yazılımlardan yaygın olarak etkilenen tüm sistemlere (özellikle kişisel bilgisayarlara ve sunuculara) dağıtın.

5.1.1: Virüsten koruma programlarının, bilinen tüm kötü amaçlı yazılım türlerin itespit etme, kaldırma ve koruma sağlama becerisine sahip olduğundan emin olun.

5.2: Tüm virüsten koruma mekanizmalarının güncel tutulduğundan, düzenli taramalar gerçekleştirdiğinden ve PCI DSS 10.7 sayılı gerekliliğe göre tutulan denetim günlükleri oluşturduğundan emin olun.

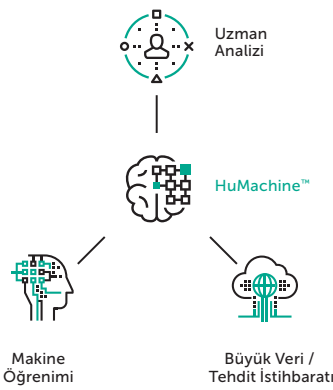
5.3: Virüsten koruma mekanizmalarının etkin bir biçimde çalıştığından ve sınırlı bir zaman dilimi için olay temelinde özel olarak yönetim tarafından yetkilendirilmediği sürece kullanıcılarca devre dışı bırakılamadığı ya da değiştirilemediğinden emin olun.

6.2: Tüm sistem bileşenlerinin ve yazılımların, satıcı tarafından sunulan uygulanabilir düzeltme ekleri yüklenerek bilinen güvenlik açıklarına karşı korunduğundan emin olun. Önemli düzeltme eklerini, yayınlanmalarından sonraki bir ay içinde yükleyin.

Virüsten Korumanın Ötesinde

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS), kredi kartı verilerini temel alan sistemlerin birçok teknik gereksinimini ve ayarlarını düzenler. Ancak, ATM'ler ve Satış Noktası cihazları için güvenlik düzenlemeleri yalnızca virüsten koruma tabanlı güvenlik konularını kapsamaktadır. Yukarıda belirtildiği gibi ve son zamanlarda gerçekleştirilen saldırılardan görülebileceği üzere yalnızca virüsten koruma tabanlı bir yaklaşım, günümüzün ATP/POS tehditlerine karşı sınırlı etkinlik sağlar. Bu nedenle, artık diğer güvenlik bağlamlarında başarısını kanıtlanmış olan Cihaz Kontrolü ve Varsayılan Olarak Reddet özelliğini kritik gömülü sistemlere uygulama zamanı gelmiştir.

Kritik ödeme sistemleri uç noktalarınızı daha etkili bir şekilde korumakla ilgili daha fazla bilgi edinmek için lütfen Kaspersky Lab Kurumsal Satış Ekibi ile iletişime geçin.



Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr