KASPERSKY lab

# Kaspersky Embedded Systems Security – ATM'leri Koruma

www.kaspersky.com.tr
#truecybersecurity

# Kaspersky Embedded Systems Security – ATM'leri Koruma

## "Küçük para kutusunun" büyük sorunları

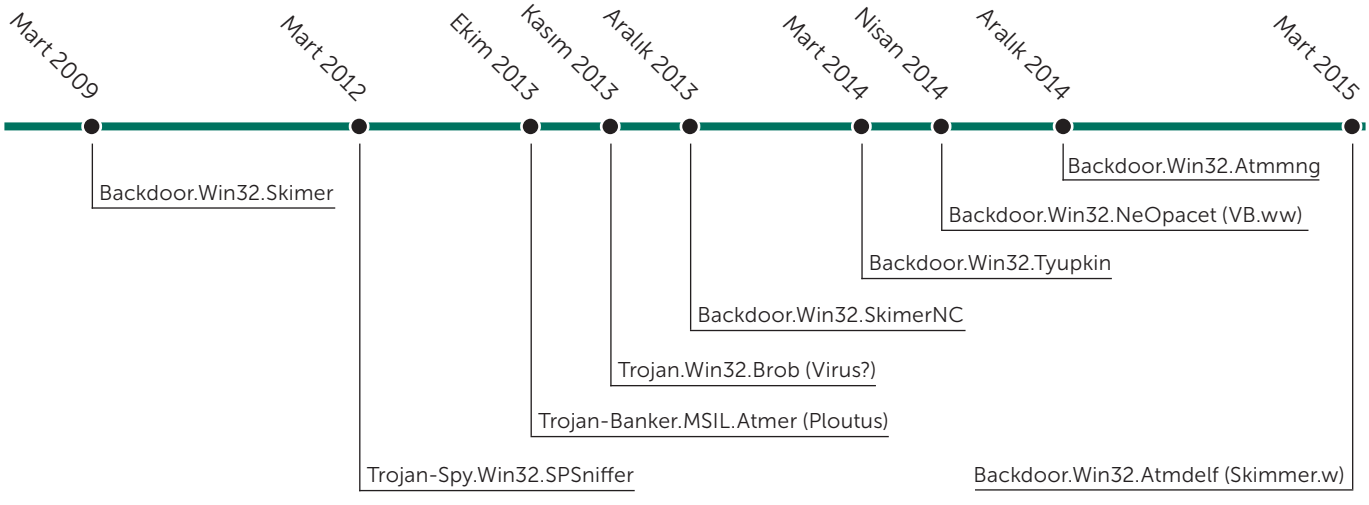
ATM'ler her zaman suçluların dikkatini çekmiştir. Saldırganlar, bu makinelerin içindeki paraya ulaşmak için matkaplar, yuvarlak testereler, pürmüzler, patlayıcılar ve bir arabanın arkasına bağlayarak çekmeye çalışmak gibi sert yöntemlere başvurmuştur (hatta hâlâ başvurmaya devam ederler).

Saldırganlar, daha sonra çeşitli kart kopyalama cihazlarına yönelmiştir. Bunlar, ATM'nin gerektirdiği banka kartı bilgilerini çalmak için özel olarak tasarlanan cihazlardır. Ancak kredi kartı ile ödeme cihazı arasındaki etkileşim için bazı gereklilikler tanımlayan uluslararası "EMV" standardının (Europay, MasterCard, VISA) uygulanmasıyla ATM aracılığıyla yapılan finansal işlemlerin güvenliği önemli ölçüde artmıştır. Sonuç olarak ATM'lerde kart kopyalama işlemi gözle görülür şekilde azalmıştır.

Ancak yine de pes etmeyen suçlular ATM'leri elektrikli araçlar veya metal halatlarla ele geçirmeye çalışmak yerine özel olarak hazırlanmış kötü amaçlı yazılımlar kullanmaya başlamıştır. Saldırganlar, artık patlayıcılara veya "beyaz plastik" bir karta (çalınan ödeme kartının verilerini içeren özel hazırlanmış bir kart) ihtiyaç duymaz. Yapmaları gereken tek şey bir ATM'ye Truva Atı virüsü bulaştırarak istedikleri anda ATM'deki tüm parayı çekmektir. Suçlular, para çalmanın yanı sıra makinenin çalışmasını kesintiye uğratabilir ve ATM'ye sahip olan bankanın finansal kayıp yaşamasına neden olacak bir DoS (Hizmet Engelleme) saldırısı başlatabilir.

Finansal kuruluşlar, yıllardır ATM'leri hedef alan çok sayıda kötü amaçlı yazılım örneğine tanık olmaktadır. Örneğin, ATM'leri hedef alan ilk kötü amaçlı yazılım, Backdoor.Win32.Skimmer, 2009 yılında Kaspersky Lab tarafından tespit edilmiştir ve hâlâ bazı makinelerde bulunabilir. Bu Truva Atı, kullanıcının banka kartı verilerini çalar ve hesap sahibinin bilgisi olmadan nakit para çekebilir.

Başka bir ilginç örnek ise Trojan-Spy.Win32.SPSniffer veya diğer adıyla Chupa Cabra yazılımıdır. Bu Truva Atı, ilk kez 2010 yılında Kaspersky Lab uzmanları tarafından Brezilya'da tespit edilmiştir. Her türlü ATM'de çalışabilen bu yazılım, kart bilgilerini okumak için para çekme makinesinden gelen verileri yakalar.




Şekil 1: ATM kötü amaçlı yazılım tespitinin zaman çizelgesi

Yıllar boyunca Kaspersky Lab olarak en yaygın numuneleri analiz etmeye ve ATM koruması için gerekli önlemleri ve teknolojileri belirlemeye yetecek kadar Truva Atı örneği biriktirdik.

# Backdoor.MSIL.Tyupkin

2014 yılının Mart ayında ATM'lere yüklenen ve suçluların büyük miktarda para çekmesine olanak tanıyan kötü amaçlı bir yazılım dünya basınına yansıdı. Saldırganın yapması gereken tek şey virüslü bir ATM'ye gitmek ve klavyeye belirli bir şifre girmekti. Bu işlemlerden sonra makine içindeki tüm parayı boşaltıyordu.

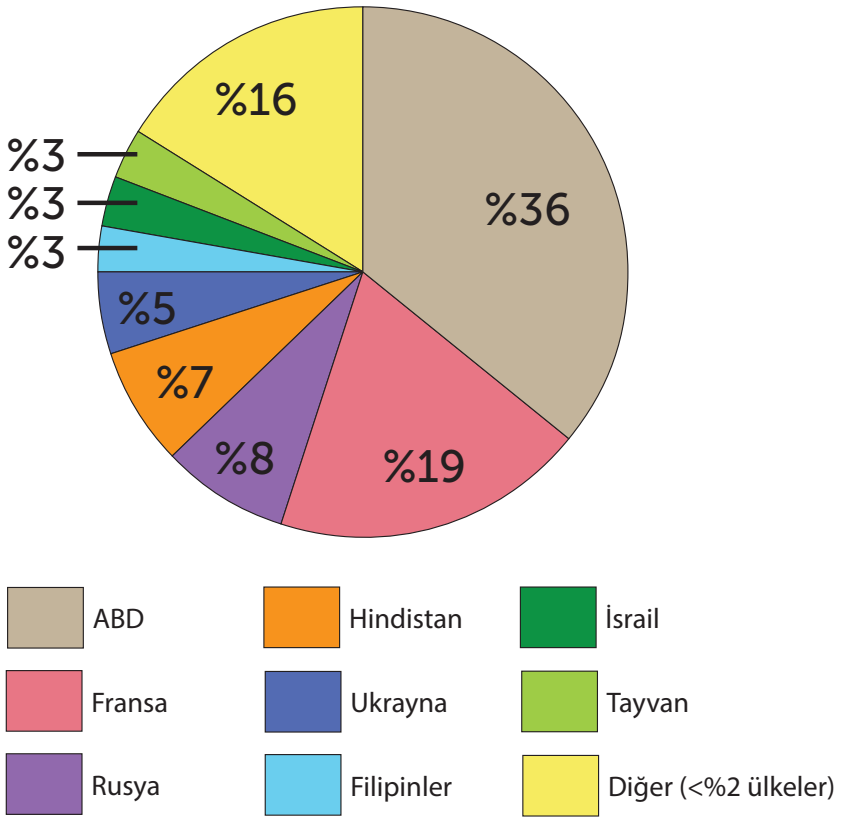
Kötü amaçlı kodun işlevselliğini ve ATM'ye nasıl girdiğini analiz etmeden önce, her ATM'nin belirli görevleri gerçekleştirmek için tasarlanmış bir bilgisayar olduğunu anlamamız gereklidir. Bu durum, ATM'lerin geleneksel iş istasyonları ve sunucularla aynı türden tehditlerle karşı karşıya olduğu anlamına gelir. ATM bilgisayarlarında çalışan işletim sistemleri masaüstü ve sunucu versiyonlarındaki güvenlik açıklarına sahip olabilir.

Kaspersky Lab uzmanlarına göre, Tyupkin kötü amaçlı yazılımı (Backdoor.Win32.Tyupkin), ATM bilgisayarına doğrudan erişimi olan bir suçlunun kullandığı çalıştırılabilir CD'nin yardımıyla ATM'lere kurulmuştur.

Kötü amaçlı yazılım, ATM'nin işletim sistemine sızdıktan sonra virüslü makinede varlığını sürdürerek suçluların makinenin içeriğine erişmesini sağlamıştır.

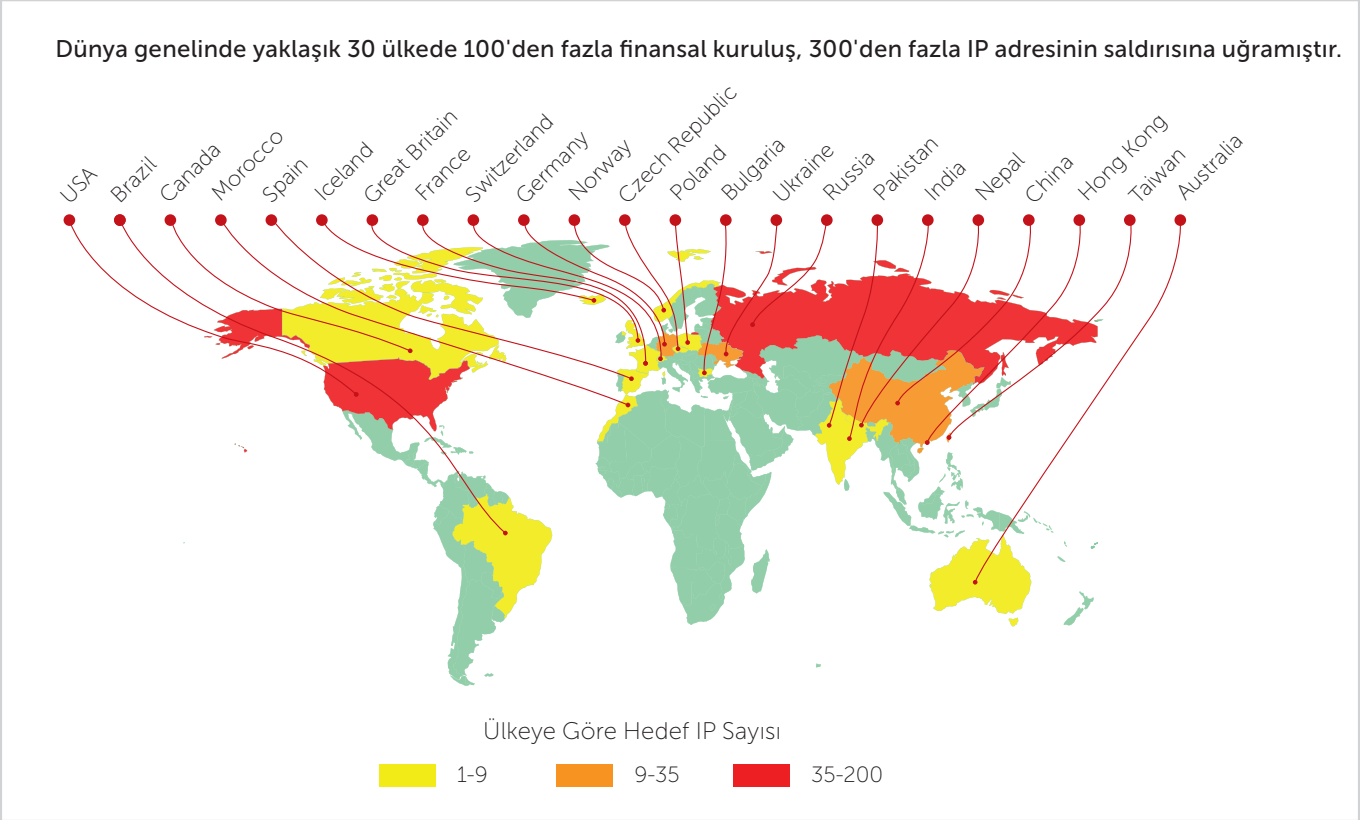
Bu Truva Atı, cihaza girdikten sonra derhal belirli bir satıcıya ait yüklü koruma çözümünü yazılım bileşenlerini kaldırarak devre dışı bırakmış, kullanıcı girdisini bekleyen bir sonsuz döngü oluşturmuş ve tespit edilmeyi önlemek için yalnızca Pazar ve Pazartesi gecelerinde yapılan komutları kabul etmiştir. Normal bir kullanıcıyla etkileşimi ortadan kaldırmak için Truva Atı'nın kabul ettiği komutları ve özel bir şifreyi kullanan suçlular, ATM kasasına erişim sağlamış ve nakit parayı çekebilmiştir.

Ancak, Tyupkin Kaspersky Lab uzmanlarının karşılaştığı ATM'lere yönelik tek tehdit değildir.




Şekil 2: Ülkeye göre Tyupkin numunelerinin sayısı (VirusTotal istatistiklerine göre)

## Carbanak hedeflerinin haritası




Şekil 3: Ülkeye göre Carbanak dağılımı

# Carbanak

Kaspersky Lab, 2014 yılında alıcı ve ATM arasında herhangi bir fiziksel etkileşim olmadan ATM tarafından nakit para verildikten sonra bir adli bilişim soruşturmasına dahil oldu. Carbanak saldırısı soruşturması ve soruşturmaya adını veren kötü amaçlı yazılım hakkındaki araştırma bu olayla başladı.

Carbanak, Carberp kodu tabanlı arka kapı yazılımıdır. Casusluk, veri toplama ve virüslü bilgisayara uzaktan erişim sağlama amaçlarıyla tasarlanmıştır. Saldırganlar banka ağındaki bir makineye erişim sağladıktan sonra virüsü işleme, muhasebe ve ATM'ler gibi kritik sistemlere yayma fırsatları yakalamak için ağı keşfetmeye başlamıştır. Bunu manuel bir şekilde istedikleri bilgisayarları (ör. yönetici bilgisayarları) ele geçirerek ve virüsü ağdaki diğer bilgisayarlara yayabilecek araçlar kullanarak gerçekleştirmişlerdir. Diğer bir deyişle, saldırganlar, ağa erişim kazandıktan sonra ilgilendikleri bir şey bulana kadar bir bilgisayardan diğerine geçmiştir. İlgilendikleri şey, saldırıdan saldırıya değişiklik gösterse de sonuç hep aynıdır. Saldırganlar finansal kuruluştan para çalar ve ATM'ler paranın çekilmesi için ana kanallarından biri olarak kullanılır.

Suçlular, dahili ATM ağına erişimi olan bilgisayarlara sızmayı başardığında veya banka kendi ATM aygıtlarına uzaktan erişim sağladığında dolandırıcılar bu durumu para çekme için kullanmıştır. ATM yazılımına sızmak için özel araçlara bile ihtiyaç duymayan saldırganlar, ATM ekipmanlarını yasal olarak kontrol etmek ve test etmek için tasarlanmış standart bir araç seti kullanmıştır.

ATM'lere yüklenen ve izleme için tasarlanmış çözümler, çoğu durumda, bankanın dahili ağındaki özel iş istasyonlarından komut alan ve daha sonra bu istasyonlara veri gönderen aracılardır. Örneğin, bu aracılar aşağıdakileri yapabilir:

- ATM içindeki olayları izleme.

- Bankanın tüm ATM'lerine yazılım dağıtma.
- ATM'lerdeki dosyaları, banka içindeki özel bir sunucuya indirme.
- ATM'lere uzaktan erişim sağlama.

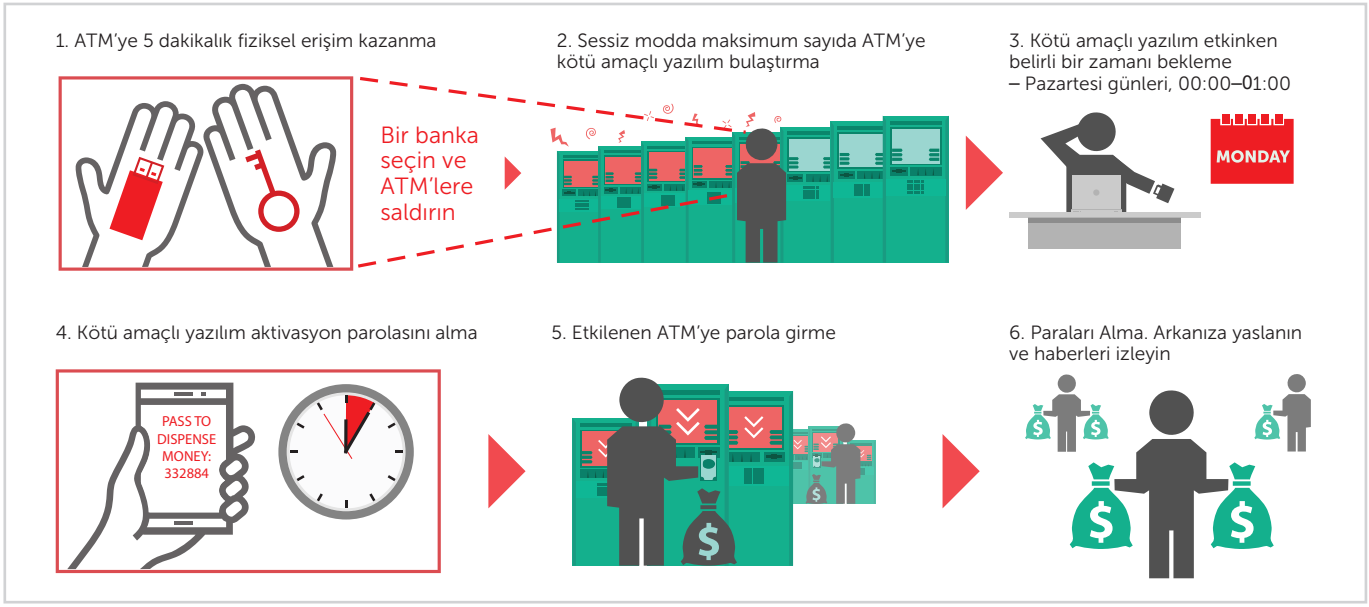
Bu aracılar, banka çalışanları tarafından ATM'lerin uzaktan yönetimi ve yapılandırılması için kullanılır ve bu nedenle genellikle ATM cihazında çalışan yazılımın "beyaz listesinde" yer alır. Dolayısıyla Carbanak saldırılarının da gösterdiği üzere bu aracılar, bankanın dahili ağına erişim sağlayan saldırganların özel ilgisini çeker.

# Gömülü Sistemlerin Güvenliği

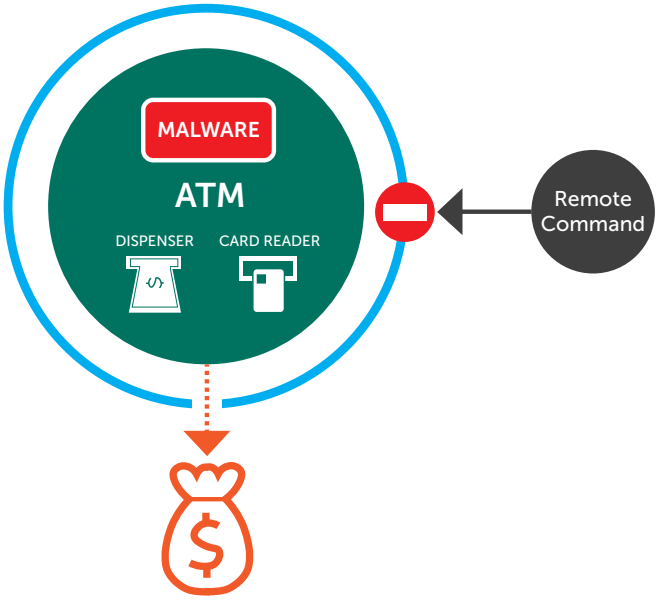
Gömülü sistem, doğrudan yönettiği cihazda yer alan özel bir bilgisayardır. Para çekme makinelerindeki gömülü sistemler, ATM'de bulunan bir kontrol bilgisayarıdır. Bu bilgisayarlar, Gömülü Windows sistemi gibi işletim sisteminin özel bir versiyonuyla çalışır. ATM'nin çalışması için bu işletim sisteminde son derece kısıtlı bir yazılım setine ihtiyaç duyulmasına rağmen bu işletim sistemi, tıpkı masaüstü ve sunucu versiyonlarında olduğu gibi güvenlik açıkları içerebilir ve bunlar için ek koruma yöntemi gereklidir.

Daha önce açıklanan Tyupkin olayları, saldırganların kötü amaçlı yazılım dosyalarını çalıştırılabilir CD-ROM'dan ATM'ye kopyalama ve çalıştırma konusunda zorlanmadıklarını göstermektedir. Bu aşamada ATM'lerin fiziksel olarak korunmasıyla ilgili önerilerin bile uygulanmayarak siber suçlulara çalıştırılabilir CD kullanma şansı verildiğini görebiliriz. Ancak, sorun yalnızca cihazın fiziksel olarak savunmasız olması değil aynı zamanda saldırganların rastgele kötü amaçlı kodu yürütebilmiş olmasıdır. Dolandırıcılar, bu kötü amaçlı kodu başlattıktan sonra içi para dolu ATM kasalarına erişim sağlayabilmiştir.

## Tyupkin saldırı şeması




Şekil 4: ATM kötü amaçlı yazılımı "Tyupkin", ATM'leri bakım moduna geçirir ve nakit para vermelerini sağlar




Şekil 5: ATM uzaktan erişim araçlarını içermese bile, suçlular yasa dışı bir şekilde para çekmek veya ödeme verilerini çalmak için kötü amaçlı yazılımlar kullanabilir

# Varsayılan Olarak Reddet yaklaşımı

Geleneksel iş istasyonları ve sunucular, uzun süredir ofis bilgisayarlarında yalnızca işle ilgili yazılımların kullanılmasını sağlayan Varsayılan Olarak Reddet yaklaşımını ve ilgili "beyaz liste" teknolojisini kullanmaktadır. Ancak, bu teknolojileri kullanan ve iş istasyonları ile sunucularda çalıştırılan geleneksel yazılım çözümleri, genellikle çok sınırlı bilgi işlem kaynaklarına sahip bir donanım üzerinde çalışan gömülü sistemler için tasarlanmamıştır. Bu durum, ATM'lerde gömülü bilgisayarlarda bulunmayan bilgi işlem kaynaklarını gerektiren mevcut güvenlik çözümlerinin kullanımına bazı kısıtlamalar getirir.

Kaspersky Lab uzmanları, gömülü sistemleri korumak için özel Kaspersky Embedded Systems Security çözümünü geliştirmiştir. Çözüm, bu tür cihazların kendine özgü özelliklerini dikkate alır ve gömülü işletim sistemlerini hedef alan siber tehditlerle mücadele etmek için "Varsayılan Olarak Reddet" teknolojisini içerir. Bu uygulama, ATM işletim sistemindeki tüm uygulamaların aşağıdaki senaryoya göre çalıştırılmasını sağlar:

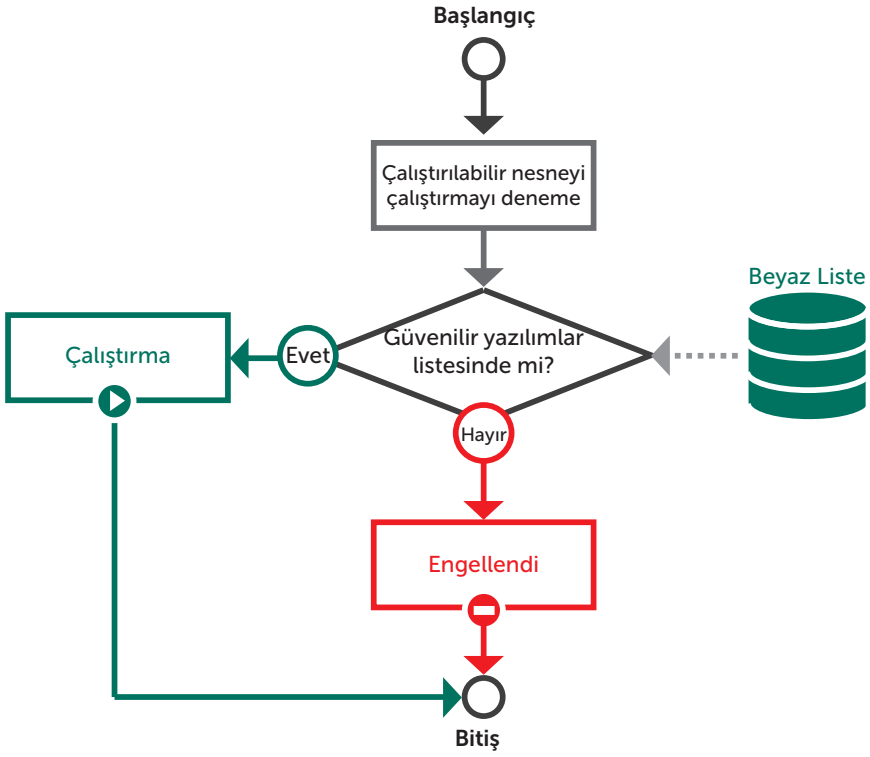
- İşletim sistemi bir uygulamanın, komut dosyasının veya kitaplığın yürütülmesini başlatır.
- Ürün güvenlik sistemi, güvenilir uygulamalardan ve bileşenlerinden oluşan beyaz listeyi kullanarak uygulamanın, kitaplığın veya komut dosyasının güvenilir olup olmadığını denetler.
- Nesne güvenilir olarak tanımlanırsa çalışmasına izin verilir.  Aksi takdirde engellenir.

"Varsayılan Olarak Reddet" teknolojisi, ATM işletim sisteminde yalnızca ATM görevlerini gerçekleştirmek için gerekli uygulamalara izin verildiği bir yazılım ortamı oluşturur. Bu sayede siber suçluların "Varsayılan Olarak Reddet" teknolojisiyle korunan ATM işletim sistemlerinde rastgele kod yürütme girişimleri başarısız olur.

# Yetkisiz indirmeleri engelleme

Ancak siber suçlular, Typukin vakasında kötü amaçlı yazılım kodunu özel bir çalıştırılabilir CD-ROM'dan indirerek çözülmesi zor bir yaklaşım kullanmıştır. Suçlular, bu yöntemle ATM işletim sisteminin dizinlerine erişim sağlamış ve dosyaları değiştirmiştir. Bu sayede daha sonra işletim sisteminin içinde çalışmak için gerekli tüm ayrıcalıkları alan kötü amaçlı kod indirilmiştir.

ATM'leri bu tür tehditlerden korumak için, kötü amaçlı bir kod içerebilecek veya siber suçluların yüklü bir koruma çözümünü devre dışı bırakmasını sağlayabilecek harici medyadan yetkisiz indirme işleminin engellenmesi gereklidir. Bu prosedür, BIOS'ta doğru yük sırasını ayarlayarak (ATM işletim sistemini sabit sürücüden yüklemek birinci sırada olmalıdır) ve BIOS ayarlarını parola ile koruyarak uygulanabilir. ATM korumasına yönelik diğer bir yaklaşım ise ATM işletim sisteminin yüklendiği diskin Tam Disk Şifrelemesi (FDE) ile korunmasıdır. Kaspersky Endpoint Security for Windows çözümünde uygulanan FDE teknolojisi, bir ATM'ye uygulandığında ATM girdi cihazına erişimi olan siber suçluların işletim sistemi dosyalarını değiştirme, ATM dosya sistemini bozma veya işletim sistemi çalıştırılırken kötü amaçlı kod başlatma girişimlerini engelleyebilir. Ancak bu mekanizmanın kullanımının, bütünlük ve cihaz kullanılabilirliği açısından belirli riskler taşıdığı göz önünde bulundurulmalıdır. Dolayısıyla bu tür cihazlarda FDE kullanımı bazı durumlarda uygun olmayabilir.




Ancak, Carbanak saldırılarının gösterdiği üzere ATM'de varsayılan olarak beyaz listeye alınan kötü amaçlı olmayan özel izleme ve uzaktan erişim araçları bile siber suçluların dahili ATM ağına erişebilen bilgisayarlara sızması durumunda tehdit oluşturabilir.

# Güvenlik için izleme

Siber suçluların ATM'lere yüklü standart araçları kullandıkları tehditlere karşı koruma sağlamak için BT güvenlik yöneticilerinin proaktif önlemler alması gerekir:

- ATM'ye uzaktan erişim olasılığını ortadan kaldırma.
- Ekipmandaki kritik tüm değişikliklerin önlenmesi (ATM cihazına uzaktan erişimi engellemek mümkün değilse en azından ATM'leri kontrol eden iş istasyonlarının kurumsal ağdan çıkarılması gerekir).
- ATM güvenliğini izlemek ve sağlamak için tek bir araç kullanma.

Bizim çözümümüzde, bu izleme aracı Kaspersky Embedded Systems Security'nin bir parçası olan Kaspersky Security Center'dır. Bu teknoloji, her ATM cihazının durumu hakkında bilgi toplar ve ATM'lere yüklenen üçüncü taraf izleme araçlarından gelen raporları destekler. Böylece ATM yöneticileri, Kaspersky Security Center'daki her cihazın durumunu analiz edebilir ve ek "ön kapıları" (Uzaktan Erişim Araçları) saldırganlara karşı kapalı tutabilir.

# ATM'lerin korunması; sonuç

ATM işletim sistemi, geleneksel iş istasyonu işletim sistemlerin tüm risklerine sahip özel bir işletim sistemi versiyonudur. ATM'ler, özel olarak geliştirilmiş bir Truva Atı'nı içeren hedefli saldırılara maruz kalmasa bile makinenin çalışmasını etkileyebilecek ve ciddi finansal kayıplara neden olabilecek standart masaüstü kötü amaçlı yazılımların bulaşma riski her zaman için geçerliliğini korur. Bu nedenle, Kaspersky Lab'in gömülü sistemlere yönelik güvenlik çözümü, yalnızca ATM'ye özgü tehditlere karşı değil, işletim sisteminde oluşabilecek ve hizmetleri kesintiye uğratabilecek kötü amaçlı yazılımların tüm biçimlerine karşı koruma sağlamak üzere tasarlanmış antivirüs teknolojilerini bir araya getirir.

Finansal kuruluşlar, para çekme makinelerinin korunması konusunda daha dikkatli olmalı ve tüm ağ altyapısının yanı sıra hem donanım bileşenlerinin hem de ATM işletim sistemlerinin güvenliğini düşünmelidir. Kuruluşlar, bunu gömülü sistemlere yönelik özel güvenlik çözümlerinin yanı sıra kurumsal ağlarda uzun süredir kullanılan koruma araçlarından faydalanarak gerçekleştirebilir. Ancak bir olay meydana geldiğinde emniyet teşkilatlarıyla ve BT güvenliğinde uzmanlaşan şirketlerle iş birliği yaparak hızlı ve etkin bir şekilde harekete geçilmesi büyük önem taşır.

# Kaspersky Lab Teknolojileri'nde uzmanlık dünyası

Kaspersky Lab ürünlerinin verimliliği, bağımsız testlerin sonuçlarıyla düzenli olarak kanıtlanır. Şirket, 2015 yılında, en iyi 3 güvenlik çözümü üreticisi sıralamasında birinciliği elde etmiştir. Birçok ülkede saygın değerlendirme kurumları tarafından düzenlenen 84 farklı testin sonuçlarına göre, Kaspersky Lab çözümleri bu testlerin %82'sinde ilk üçe girerken 60 kez birinci olmayı başarmıştır. Bu test sonuçları, Kaspersky Lab'in sektördeki en iyi korumayı sağladığına dair inkâr edilemez bir kanıt sunar.

# Kaspersky Lab Hakkında

Kaspersky Lab, 1997 yılında kurulan global bir siber güvenlik şirketidir. Kaspersky Lab'in derin tehdit istihbaratı ve güvenlik uzmanlığı sürekli olarak, dünya çapındaki işletmeleri, kritik altyapıları, devletleri ve tüketicileri koruyan güvenlik çözümleri ve hizmetleri şeklinde ortaya çıkar. Şirketin kapsamlı güvenlik portföyü, karmaşık ve gelişen dijital tehditlerle mücadele için lider uç nokta korumasını ve birçok özelleştirilmiş güvenlik çözümünü içerir. Kaspersky Lab teknolojileri, 400 milyondan fazla kullanıcıyı korumaktadır. Ayrıca 270.000 kurumsal müşterimizin en önemli varlıklarını korumalarına yardımcı oluruz.

Daha fazla bilgi için şu adresi ziyaret edin: http://www.kaspersky.com/enterprise

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

#truecybersecurity
#HuMachine

**www.kaspersky.com.tr**