Siber güvenlikte Makine Öğrenimi Dönemi:

Daha güvenli bir dünyaya doğru bir adım mı, yoksa kaosun başlangıcı mı?

Ondrej Kubovič, ESET Güvenlik Farkındalık Uzmanı

katkıda bulunanlar

Juraj Jánošík, ESET AI/ML ekibi Başkanı

Peter Košinár, ESET Teknik Araştırmacısı

İçindekiler

GİRİŞ

Yapay zeka (AI) fikri ve makine öğreniminin (ML) gerçek uygulamaları yıllardır çeşitli alanları etkiliyor olsa da, bunların dönüştürücü potansiyelleri henüz tam olarak ortaya çıkmadı.

ML-tabanlı teknolojiler büyük ölçekli dolandırıcılıkla mücadele etmeye, iş süreçlerini değerlendirmeye ve optimize etmeye, test prosedürlerini geliştirmeye ve mevcut sorunlara yeni çözümler geliştirmeye yardımcı olmaktadır. Ancak çoğu yenilik gibi, makine öğreniminin de bazı dezavantajları bulunmaktadır.

Saldırganlar bu teknolojinin sunduğu fırsatlarla birlikte gerçek değerinin de farkındadır ve bunları kendi çıkarları için kötüye kullanmaktadırlar. Makine öğrenimi, henüz değilse bile yeni kötü amaçlı yazılım türlerinin ortaya çıkmasını tetikleyecek, belirli kurbanları hedef alarak değerli bilgiler elde edebilecek, sıfır gün açıklarını tespit edebilecek ve siber suçluların kendi altyapılarını (botnetler gibi) koruyabilecek.

Tüm bunların yanı sıra, meşru kuruluşlar tarafından konumlandırılan ML çözümleri de ilgi çekici birer hedef haline gelecekler. Saldırganlar zehirli veri kümeleri oluşturmak suretiyle bu faydalı sistemleri manipüle edip zorlayarak yanlış kararlar vermelerine ve izlenen ortamın çarpık bir görünümünü sunmalarına neden olup hasar, kaos ve bozulmaya sebebiyet verebilmektedirler.

Makine öğreniminin hangi etkilerinin olumlu ya da olumsuz olacağını söylemek zordur. Ancak şu an gördüğümüz şey, ML destekli sistemlerin önlenemez şekilde büyümesi sonucu siber güvenlik dağılımının her iki tarafında da tüm internet güvenliğinin geri dönülemez şekilde değiştiğidir.

Bu doküman, makine öğrenimi teknolojisinin çeşitli alanlarda neden olduğu hareketliliği ve kurumsal karar vericileri nasıl etkilediğini açıklamayı amaçlamaktadır. Ayrıca ML kullanımının güçlü göstergelerine sahip, dolaşımda gözlenen siber saldırıları da özetlemektedir. Son olarak, ESET'in makine öğrenimine olan yaklaşımını ve bunları mevcut ürünlerindeki uygulamalarını göreceğiz.

Yapay Zeka

Bu, insan müdahalesi olmadan, yalnızca çevreden topladığı verilerle karar alabilen ve bağımsız olarak öğrenebilen, genel anlamıyla akıllı ve kendine yetebilen bir makinenin henüz ulaşılamaz idealini temsil etmektedir.

Makine Öğrenimi

Veri işleme algoritmaları, bilgisayar sistemlerinin büyük miktardaki verilere ait örnekleri ve anomalileri tespit etmek amacıyla seçilen görevler yürütmesini sağlayarak, karmaşık veriyi "model" olarak da bilinen bütünleştirilmiş bir şekle dönüştürmektedir. Nihai amaç olan gerçek AI oluşturulmadan, makine öğrenimi bunun gerçekleştirilmesinde kilit rol oynayacak teknolojilerden biri olarak kabul edilmektedir.

Derin Öğrenme

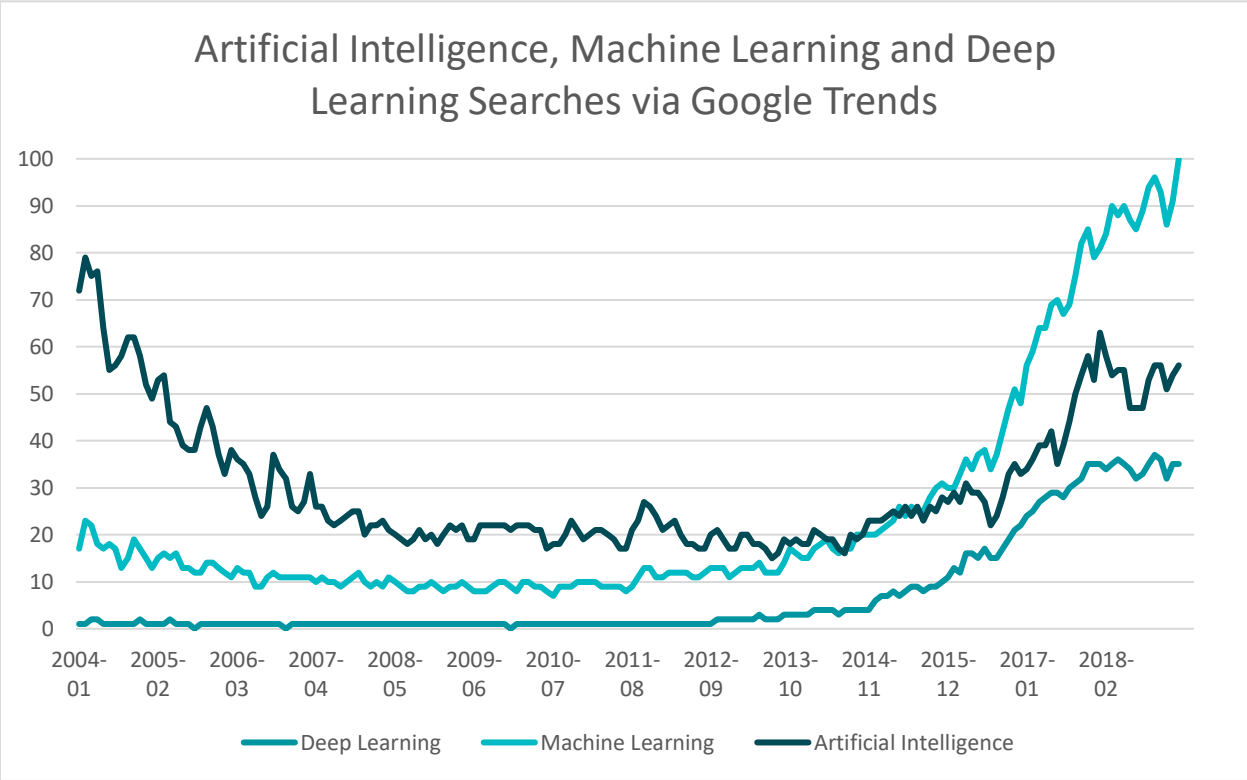
Makine öğrenimi modellerinin bir alt kümesi olarak, insan beyninden esinlenerek oluşturulmuş, büyük sıralı veri setlerinin işlenmesinde etkili olduğu kanıtlanmıştır. Derin öğrenme siber güvenlik alanında önemli gelişmeler sağlamıştır. Tespit yeteneklerine sağladığı katkı, sabit duran bir resimle yüksek kaliteli bir video kaydına bakmak arasındaki farka benzetilebilir.

AI HAREKETLİLİĞİ VS. MAKİNE ÖĞRENİMİ GERÇEĞİ

Günümüzde Yapay Zeka, esasen moda olmuş bir sözcüktür. Genel anlamıyla akıllı makine fikri şu an için uzak bir ihtimal olsa da, parlak satış ve pazarlama malzemeleriyle oldukça uyumludur.

Diğer taraftan, "makine öğrenimi"(ML) ve onun en yaygın yöntemi "derin öğrenme", sağlam teknik ve bilimsel temellere dayanmakla birlikte, halihazırda günlük yaşantımızın bir parçası haline gelmiştir ve artarak ilgi çekmeye devam etmektedir.

Gösterilen ilgi açısından gerçek dünyadaki ML ve DL teknolojisi ile ideal AI fikri, 2014 yılından beri Google aramalarında da iyi bir şekilde belgelenmiştir (bkzŞekil1).



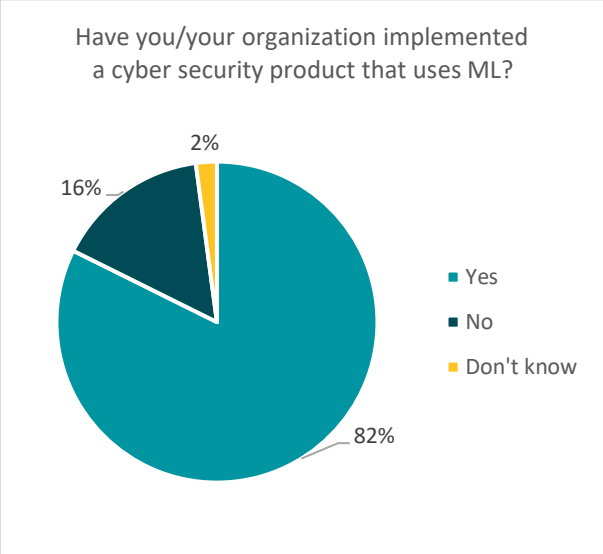
Şekil1: "Yapay Zeka", "Makine Öğrenimi", "Derin Öğrenme" terimleri için 2004-2019 yılları arasındaki arama trendleri: Google Trends

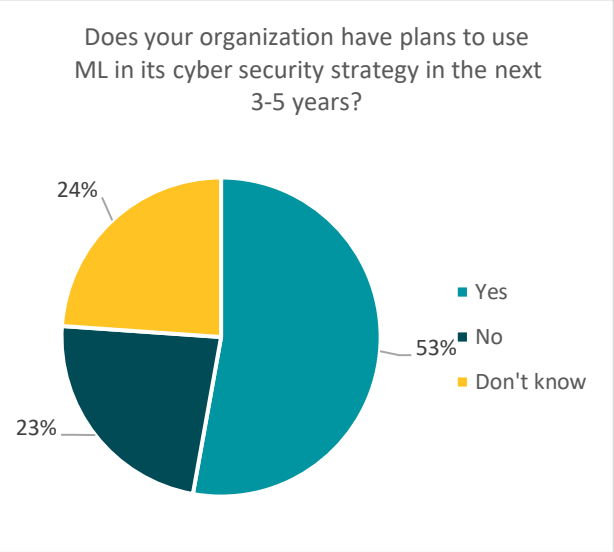
Bu eğilim makine öğreniminin sadece bilinen bir terim değil (yanlış bir şekilde sıklıkla AI ile karıştırılmakta), aynı zamanda yaygın olarak kabul edilen bir teknoloji olduğunu ifade etmekte ve iş hayatına da geçiş yaptığını ortaya koymaktadır. OnePoll tarafından ESET adına gerçekleştirilen araştırma şunları göstermiştir:

- Katılımcıların[1] %82'si**, kuruluşlarının ML kullanan bir siber güvenlik ürününe sahip olduğuna inanıyor**

[1] ABD, İngiltere ve Almanya'da yer alan, 50'nin üzerinde çalışana sahip çeşitli şirketten 900 BT yöneticisi

- Geriye kalan %18'i oluşturan katılımcıların **yarısından çoğuysa (%53)**, kuruluşlarının **3 ila 5 yıl içerisinde makine öğrenimi kullanan bir siber güvenlik ürününe geçiş yapmayı planladığını ifade ediyor.**
- Katılımcıların yalnızca %23'ü yakın gelecekte ML tabanlı bir siber güvenlik çözümü kullanmayı düşünmediklerini belirtiyor

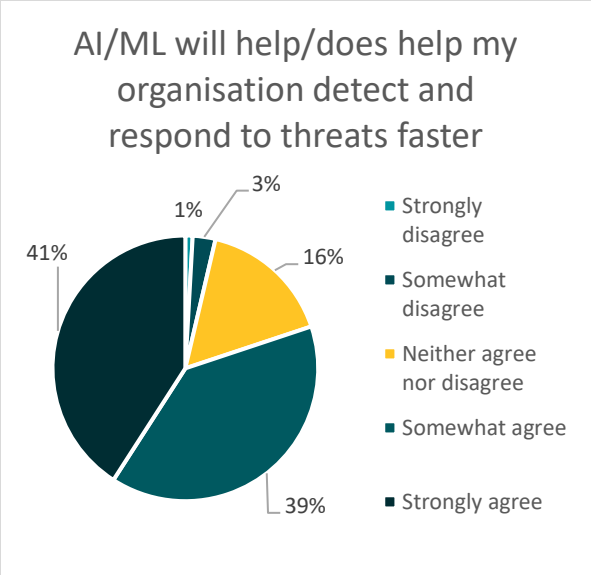


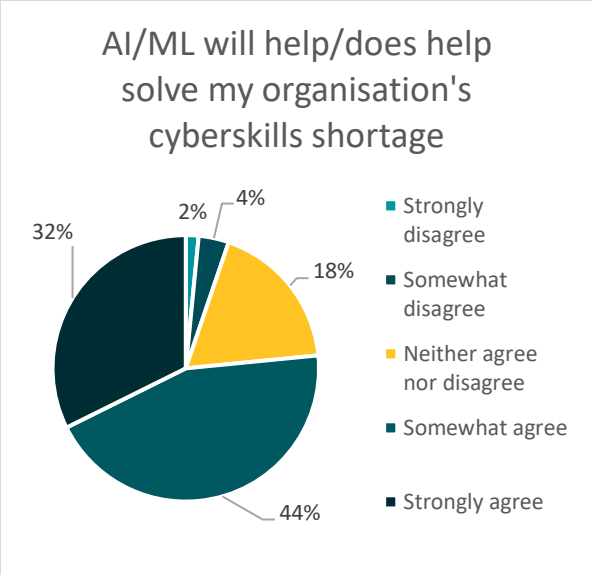


Şekil 2: Araştırma katılımcılarından halihazırda ML tabanlı bir siber güvenlik çözümü kullananların yüzdesi

Şekil 3: : Araştırma katılımcılarından ML'yi 3 ila 5 yıl içerisinde siber güvenlik stratejilerinin bir parçası olarak kullanmayı planlayanların yüzdesi

- **Ayrıca** katılımcıların %80'i, ML'nin bir noktada kuruluşlarının **tehditleri daha hızlı tespit ederek tepki vermelerine yardımcı olduğuna ya da olacağına inanıyor.**
- Katılımcıların **%76**'sı, bu teknolojilerin kesinlikle **işyerlerindeki siber güvenlik becerisi açığını kapamaya yardımcı olacağında hemfikir**





Şekil 4: AI/ML'nin tehditleri daha hızlı tespit edip onlara karşı daha hızlı tepki vermelerini sağladığını/sağlayacağını düşünen katılımcıların yüzdesi

Şekil 5: AI/ML'nin siber güvenlik becerisi açığını kapadığını/kapayacağını düşünen katılımcıların yüdesi

Yapay Zeka, ML ve DL etrafındaki pazarlama hareketliliği sonucu, katılımcıların çoğu bu teknolojilerin siber güvenlik sorunlarını çözmenin anahtarı olabileceğini düşünüyorlardı; ancak çoğu da bu teknolojilerin savunma altyapılarında uygulanmasıyla ilgili aşırıya kaçan gerçek dışı bir reklam yapıldığını kabul etmekte.

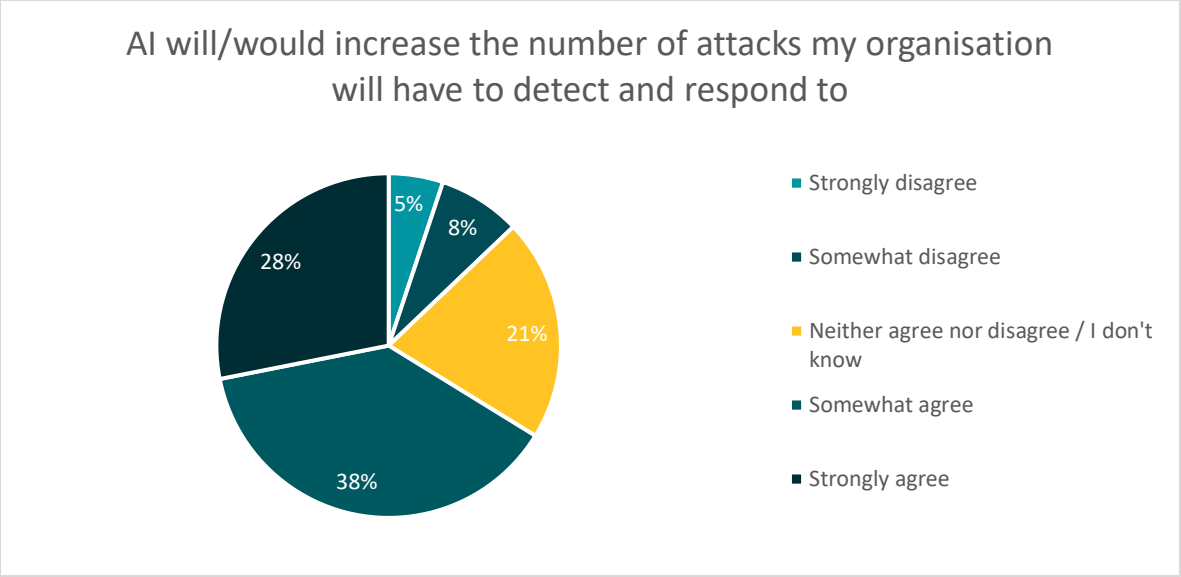
Dolayısıyla, siber suçla mücadelede bir araç olarak ML'nin değerini düşürmeden dikkate alınması gereken bazı sınırlamalar vardır; tek bir teknolojiye güvenmenin kötü sonuçlara yol açabilecek potansiyele sahip bir risk olduğunu göz önünde bulundurmak gibi.

Bu özellikle, bir saldırganın kararlı, gereken maddi imkanlara ve zamana sahip olduğu durumlarda, yalnızca ML tabanlı bir güvenlik çözümünü aşmak için bir yol bulabileceği anlamına gelmektedir. Bu nedenle, kurumsal siber güvenlikte benimsenmesi gereken daha güvenli ve dengeli bir yaklaşım, makine öğreniminin gücünü ve potansiyelini kullanabilen, ancak diğer algılama ve önleme teknolojilerini ve insan uzmanlığını da destekleyen çok katmanlı bir çözüm kullanılmasıdır.

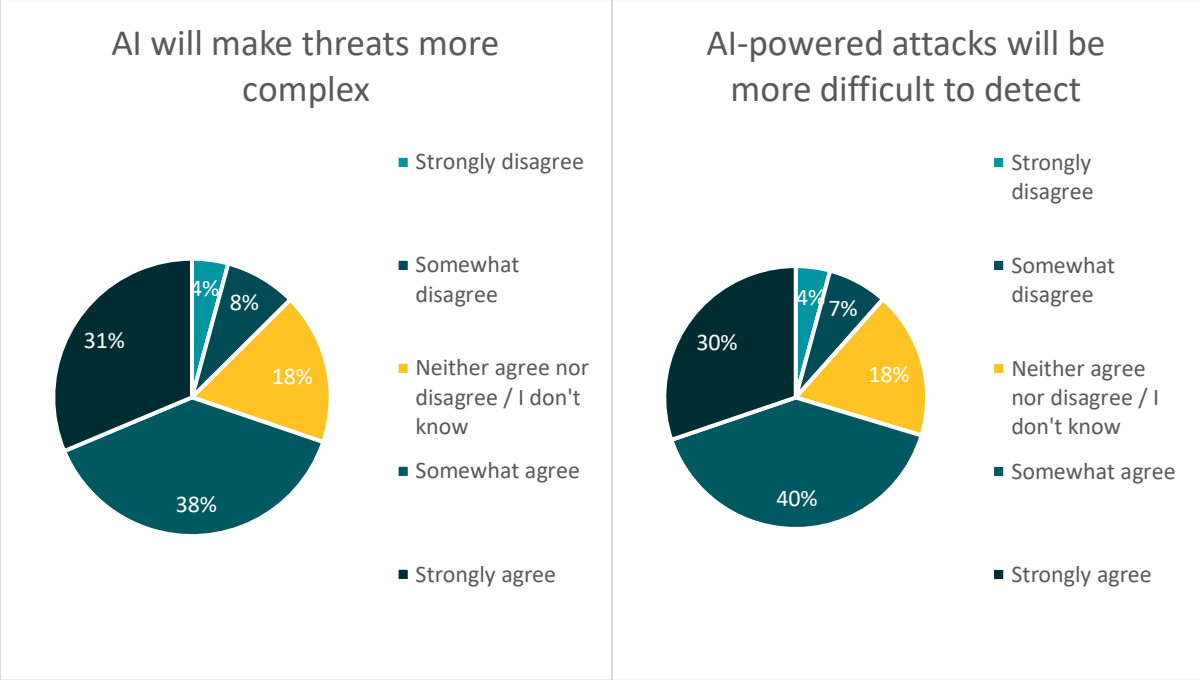
GELECEKTEKİ SİBER SALDIRILARIN KAYNAĞI ML Mİ OLACAK?

Yukarıda görüldüğü gibi, makine öğrenimi güvenlikçiler için muazzam bir dönüştürücü potansiyele sahiptir. Ne yazık ki, siber suçlular da yeni hedeflerinin farkındalar. Bir OnePoll araştırmasına göre, bu aynı zamanda kuruluşların güvenliğinden sorumlu olan pek çok yönetici ve BT çalışanı için de bir endişe kaynağı:

- Katılımcıların **%66'sı** büyük ölçüde veya bir şekilde yeni **ML uygulamalarının (teknolojilerinin) kuruluşlarındaki saldırı sayısını artıracağını düşünüyor**
- Daha da fazla katılımcı**, ML teknolojilerinin tehditleri daha karmaşık ve tespit edilebilmesi zor hale getireceğini düşünüyor** (sırasıyla **%69** ve **%70**).



Şekil 6: AI kuruluşumuzun tespit ederek tepki vermesi gereken saldırı sayısını artıracak/artırabilir



Şekil 7: AI ile tehditlerin daha karmaşık hale geleceğini düşünen katılımcıların yüzdesi

Şekil 8: AI tabanlı saldırıların tespit edilmesinin daha zor olacağını düşünen katılımcıların yüzdesi

Bu endişelerin bazıları 2003 sonlarından itibaren ortaya çıkmaya başladı. Swizzor Truva atı, her bir kurbana kötü amaçlı yazılımın polimorfolojik olarak değiştirilmiş bir varyantını ileten zararlı yazılımları dakikada bir kez yeniden paketlemek için otomasyon kullandı. Swizzor bu gelişmeler sonucu, ister otomasyon ister makine öğrenimi olsun, yeni teknolojilerin siyah şapkalılar tarafından kullanılabileceğini gösterdi.

Sonuç olarak, ESET uç nokta ürünleri gibi modern kötü amaçlı yazılım önleme çözümleri, ESET DNA Detections gibi gelişmiş algılama mekanizmaları da bunlara eklendiğinde, ML kullanan saldırılar da dahil olmak üzere ortaya çıkan tehditlerin algılanmasına, engellenmesine ve azaltılmasına olanak tanır.

Makine öğrenimi güvenlik tedbirlerinin bir parçası olmadan, ML destekli saldırılar olması durumunda da benzer sonuçlar ortaya çıkabilir. Bir algoritma, konumlandırılan güvenlik çözümünün sınırlarını öğrenmeyi kolaylaştırabilir ve saldırganların zararlı yazılımın kodunu tespitten kaçabilecek ölçüde değiştirmelerine yardımcı olabilir.

SALDIRGANLARIN ELİNDE MAKİNE ÖĞRENİMİ

DÜŞMANLAR TARAFINDAN GELECEKTEKİ OLASI KULLANIMLARI

Siber saldırganların ML tabanlı teknolojileri kendi çıkarları doğrultusunda kullanmalarının pek çok yolu vardır. Aşağıdaki bölümde, makine öğrenimi kullanımının mümkün olduğu veya beklendiği alanlardan bazıları özetlenmektedir. ML şu amaçlar için kullanılabilir:

Zararlı içerik oluşturma ve geliştirme

- Eski zararlı yazılımın önceden görülmüş otomasyon kullanılarak yeni türevlerini üretmek amacıyla geliştirilmesi ve yeniden icat edilmesi sonucu **yeni zararlı yazılım oluşturulması** Yeni oluşturulan tür, daha zor tespit edilebilen eski türevlerinin bir karışımı olabilir ve böylece benzer karakteristik özelliklere sahip yeni bir zararlı yazılım üretilmiş olur
- geçmişteki başarılı kampanyaların deneme setleri baz alınarak **oluşturulmuş yeni zararlı spam ve kimlik avı içeriği**
- **spamcılara/kimlik avcılarına zararlı içerikte kendini tekrar eden kalıpları belirlemeleri konusunda** yardımcı olur. Bu özellikler kaldırılarak ve yeni içerik rasgele bir duruma getirilerek, istenmeyen posta ve kimlik avı tehditlerinin saptanması daha zor hale gelir.

Kendini koruma

- botnetlerde olası honeypot veya araştırmacı makine olabilecek inaktif, tuhaf veya bir şekilde anormallik sergileyen makineleri tespit ederek **suçlunun altyapısındaki ele geçirilmiş/enfekte edilmiş nodların korunmasına yardımcı olmak**
- zararlı yazılımın/ saldırganın amacını ortaya çıkarabilecek **bilinen/bulunabilir uyarı işaretlerini tespit etme**
- belirli koşulları oluştuğunda etkinleştirilen, **zararlı yazılımın kendini yok etme mekanizmasının bir parçası olma**
    - *Örneğin, standart olmayan kullanıcı profili veya bir program tarafından oturum açıldığı tespit edilirse, kötü amaçlı yazılım otomatik olarak kendi kendini imha mekanizmasını etkinleştirir; böylece algılama ve daha fazla analiz imkansız hale gelir.*
- diğer kötü amaçlı kişileri/grupları işaret eden **yanlış uyarılar oluşturarak** araştırmacıları ve uzmanları aldatma
- **zararlı etkinliği gizlemek** içinkurbanın ağında **meşru ağ trafiği modellerini** taklit etme

Kötü amaçlı yazılıma ve diğer zararlı faaliyetlere yönelik "iyileştirmeler"

- veri hırsızlığı gibi durumlarda kritik öneme sahip olabilecek şekilde **saldırının hızını artırma** Algoritmalar, korunan sistemlerden hedeflenen verilerin bir insanın yapabileceğinden çok daha hızlı çıkarılmasını sağlayarak tespit edilmeyi zorlaştırır ve bunun önlenmesini neredeyse imkansız hale getirir.
- herkese açık, toplanmış veya başka bir şekilde ayıklanan verilere dayalı kurbanların profilini oluşturarak **kötü amaçlı yazılımların hedeflemesini iyileştirme**
- Geçmişten gelen en etkili yaklaşımları soyutlayarak, değerlendirerek ve önceliklendirerek gelecekteki saldırılarda kullanılmak üzere bunların birleştirileceği **en etkili saldırı tekniğini bulma** Vektörlerden birinin savunucular tarafından etkisiz hale getirilmesi durumunda, saldırganın yalnızca algoritmayı sıfırlaması, güncellenmiş girdiyle beslemesi ve farklı bir öğrenme sürecini izlemeye zorlaması gerekir.

- ML algoritmasının yeni güvenlik açıklarını bulabilmek üzere gerekli bir yöntem kullanmayı öğrenebilmesi amacıyla, yukarıdaki noktaları bulandırarak (örn. algoritmayı geçersiz, beklenmedik veya rasgele veri girdileriyle oluşturarak) **yeni sıfır-gün açıklarının bulunması**
- Giden iletişime gerek kalmadan, ağdaki rollerine göre bir botnet'teki enfekte olmuş makineler arasında **çeşitli görevler atayın**
- **Botnet'teki nodların topluca öğrenim yapabilmelerini ve en etkili saldırı formunu belirlemek için bu bilgiyi kullanmalarını sağlayın**
    - *Örneğin, ele geçirilmiş botların her biri farklı sızma tekniklerini test edebilir ve sonuçları tüm botnet'e rapor edebilir. Toplanan bilgiler, kötü amaçlı kişilerin hedeflenen altyapı/ağ hakkında daha kısa bir zaman diliminde daha fazla bilgi edinmelerine yardımcı olabilir.*

Makine Öğrenimi vs Nesnelerin İnterneti

Nesnelerin İnterneti (IoT) alanı, kuruluşundan bu yana pek çok sorunun odağı olmuştur. Yönlendiriciler, güvenlik kameraları ve çeşitli denetleyicilere benzer cihazların sayısı oldukça hızlı artmaktadır. Bununla birlikte, güvenlikleri bilinen bir şekilde eksiktir ve varsayılan cihaz bilgilerinin brute force yoluyla aşılması veya çok eski güvenlik açıklarının kötüye kullanılması gibi en ilkel sömürü tekniklerine karşı dahi duyarlıdırlar. Tüm bunlar zararlı yazılımın kolay bir şekilde içeri sızmasına olanak tanır.

Bu tür kötü amaçlı kampanyalar 2019'da yeni birer olay değildi, ancak ML tabanlı teknoloji, saldırganların oyununu bir sonraki seviyeye taşıyabilir. Birkaç olası senaryo ortaya koymak gerekirse, ML algoritmaları şunları yapabilir:

- Yukarıda açıklananla benzer şekilde,**IoT cihazlarındakisıfır gün açıklarını tespit edebilir**.
- IoT cihazları, ML'yi **gelişmiş gizlilik mekanizmaları tasarlamak** amacıyla eğitmek için kullanılabilecek çok sayıda meşru trafik bilgisi ve kullanıcı alışkanlığı barındırması açısından ideal bir platform niteliğindedir.
- Belirli cihazlara (veya gruplarına) yönelik standart süreçleri ve davranışları öğrenerek **rakip kötü amaçlı yazılım ailelerini/varyantlarını kolayca tanımlama, kaldırma veya kötüye kullanma**
- Her yıl sızan milyarlarca parola sayesinde saldırganlar, kolayca en etkili parolalardan oluşan bir deneme seti oluşturabilirler **Set üzerinde eğitilmiş ML**, diğer benzer IoT cihazlarına yönelik **gelecekteki sızma denemelerinde yeni kimlik bilgileri adayları oluşturabilir**

GÖRÜLEN OLAYLAR

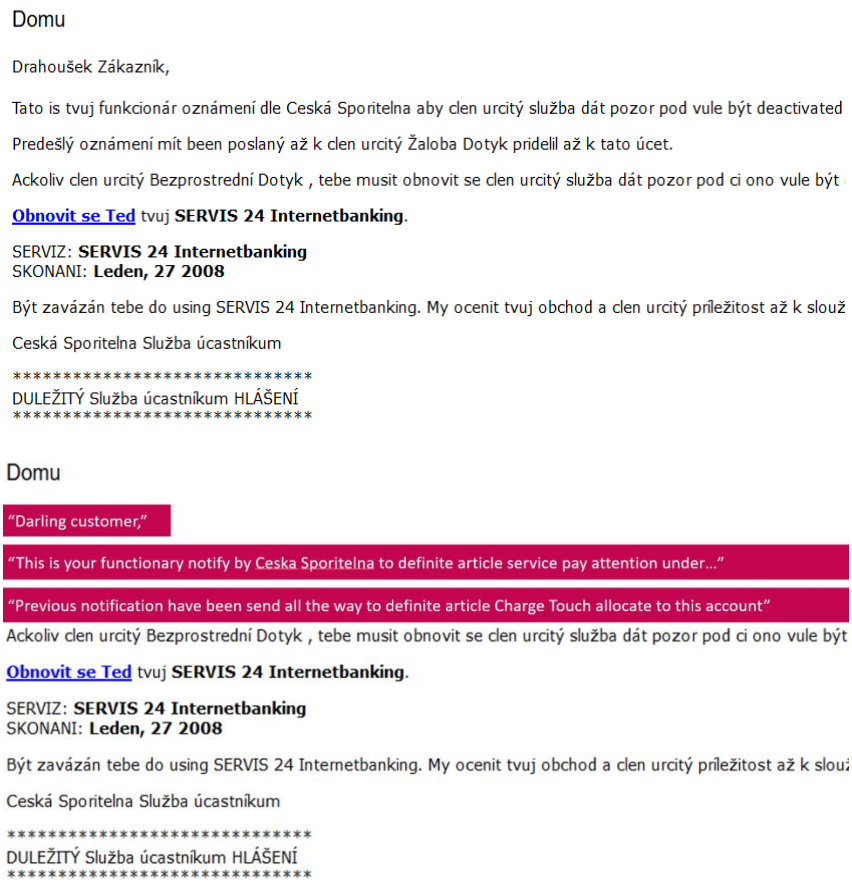
Ne yazık ki, makine öğreniminin düşmanca kullanımı da dahil olmak üzere, gelecekteki senaryoların başımıza gelecek şeylerin yalnızca başlangıcı olması gerekmiyor. ESET araştırmacıları tarafından naaliz edilen bazı mevcut olaylar, ML tabanlı teknolojilerin zaten devrede olabileceğini gösteriyor.

SPAM

Makine öğreniminin zararlı araçların “kalitesini” tartışmasız biçimde geliştirdiği bir alan spam (istenmeyen e-posta) ve kimlik avıdır. Bu sosyal mühendislik teknikleri, alıcıyı zararlı eylemlere yönlendirme becerilerine dayanmaktadır. Kurbana ulaşan e-posta dört yaşındaki bir çocuk yanlışlıkla klavyeye basmış gibi yazıldığından bu etkili bir yaklaşım değildir.

İngilizce yazılan spamlar, yıllardır düzgün bir dilbilgisi ve yazım tarzından yoksun. Bununla birlikte, diğer yerel ve bölgesel dillerde yazılan kötü amaçlı e-postalar, bu alandaki kelime ustalığının çok daha yavaş gelişmesine neden oldu. Ta ki makine öğrenimi işin içine girene kadar. Birçok çevrimiçi çeviri hizmeti ML teknolojisini motorlarına dahil etti, böylece farklı bölgelerdeki İngilizce kaynaklarını yerelleştirmede daha iyi hale geldiler. Bu durum firmalar ve düzenli kullanıcılar da dahil olmak üzere interneti kullanan herkese yardımcı oldu; aynı zamanda spamcılara ve dolandırıcılara da.

ESET bir Slovak şirketi olduğundan, bu gelişmenin örnekleri olarak Çek ve Slovak dillerini kullanacağız. Eski spam mesajları (Şekil 9) saçma kelimeler, başlangıç seviyesindeki dilbilgisi hataları, hiçbir aklı başında kuruluşun talep etmeyeceği gereklilikler gibi pek çok şeyi bir araya topladığından çıplak gözle kolaylıkla tespit edilebilmekteydi.


Domu

Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated

Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.

Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být

Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.

SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 27 2008**

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k slouž

Ceská Sporitelna Služba úcastníkum

****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****

Domu

"Darling customer,"

"This is your functionary notify by Ceska Sporitelna to definite article service pay attention under..."

"Previous notification have been send all the way to definite article Charge Touch allocate to this account"

Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být

Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.

SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 27 2008**

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k slouž

Ceská Sporitelna Služba úcastníkum

****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****

Şekil 9: Bir Çek bankasının müşterilerini hedef alan , saçma sapan dilbilgisi hatalarıyla dolu eski e-posta.

Buna karşılık, artık pek çok kuruluşun gelen kutularına düşen kaliteli spam mesajları çok daha profesyonel ve güvenilir görünüyor. Yakın tarihli bir örnekte (Şekil 10), meşru bir firmanın adını, logosunu ve adresini farklı şekilde kullanan bir fatura talebi dolandırıcılığı görülüyor. Neredeyse hiçbir yazım hatası olmadan yazılmıştır; muhtemelen çevrimiçi bir çeviri aracıyla kalitesi artırılmıştır.

From: ACG GmbH & Co. KG <f.brunner@acg-technologies.de>
Sent: Thursday, August 2, 2018 3:04 PM
Subject: INVOICE-RFQ-0094-8002-008-0018LT

Pane,

Moja kolegyňa, ktorá má túto objednávku vybavovať, je na dovolenke.

Chcem potvrdiť údaje v tejto faktúre od vás, pred jej odovzdaním na naše oddelenie účtovníctva.

Sú podrobnosti účtu na priloženej faktúre vaše správne bankové údaje?

Ak existuje nejaká chyba, ktorá potrebuje opravu v tejto faktúre?

Potvrďte kód IBAN a swift kód.

Ak by existovala akákoľvek existujúca dohoda, dajte mi vedieť.

S Pozdravom.

(Alexander Renga)

ACG GmbH & Co. KG

ACG GmbH & Co. KG
Automation Co & GmbH,
Erlenstraße 2,
60325 Frankfurt am Main,

From: ACG GmbH & Co. KG <f.brunner@acg-technologies.de>
Sent:
Subject: INVOICE-RFQ-0094-8002-008-0018LT

Sir,

My colleague, who is in charge of the order, is out of office.

I would like to confirm the order details before I hand it over to our accounting department.

Are the banking details of the attached invoice correct?

Ak existuje nejaká chyba, ktorá potrebuje opravu v tejto faktúre?

Potvrďte kód IBAN a swift kód.

Ak by existovala akákoľvek existujúca dohoda, dajte mi vedieť.

S Pozdravom.

(Alexander Renga)

ACG GmbH & Co. KG

ACG GmbH & Co. KG
Automation Co & GmbH,
Erlenstraße 2,
60325 Frankfurt am Main,

Şekil 10: Fidye yazılımları dağıtmaya çalışan güncel bir spam e-postası.

Eğitimli bir çalışan için bozuk kelime düzeni veya bu tür taleplerin tipik olarak sadece finans departmanına gönderilmesi gibi dolandırıcılığı gözler önüne seren birkaç işaret her zaman bulunmakta. Ancak benzer e-postalar günlük olarak gönderildiğinde, fidye yazılımı tarafından şifrelenmek yalnızca birkaç talihsiz tık uzakta olabilir.

EMOTET

Dolaşımda görülen ve ML benzeri izler taşıyan bir başka yaygın örnek ise modüler Truva atı indiricisi Emotet'tir. ESET araştırmacıları, bu zararlı yazılım ailesinin belirli kurbanları hedefleyebilmek adına makine öğrenimini kullandığından şüpheleniyor. Günde binlerce cihaza saldırarak onları ele geçirmesine

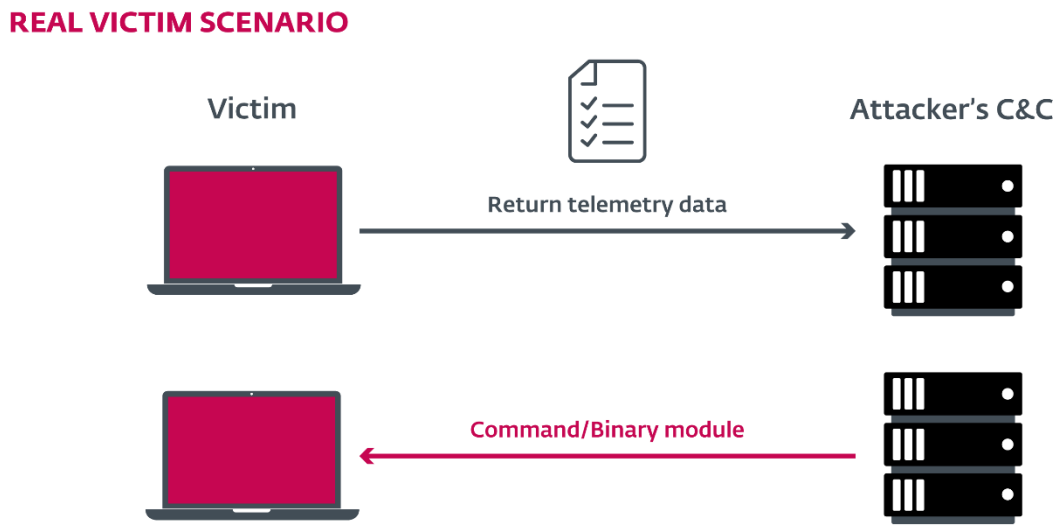
rağmen araştırmacı makinelerinden, honeypot ve botnet izleyicilerinden kaçınma konusunda oldukça etkilidir.

Emotet bunu başarmak için potansiyel kurbanlarının uzaktan ölçüm verilerini toplayarak bunları analiz için saldırganların C&C sunucularına gönderir. Bu girdilere dayanarak, kötü amaçlı yazılım sadece son yüke dahil edilecek modülleri seçmekle kalmaz, aynı zamanda gerçek insan operatörlerini sanal makinelerden ve araştırmacılar tarafından kullanılan otomatik ortamlardan da ayırt eder.

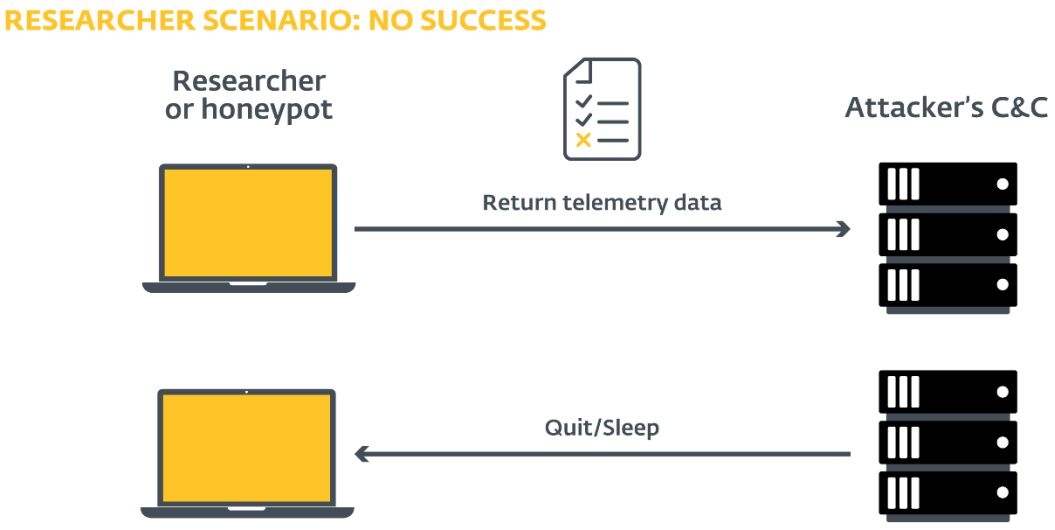
Şaşırtıcı olan, Emotet'in meşru süreçlerle tuzak niteliğindeki yapay süreçleri ayırt edebilmesidir. Yapay olanlar genelde ilk başta kabul edilirler; fakat ilk temasın ardından birkaç saat içerisinde kara listeye alınırlar. Kurbanlara yönelik kullanılacak ikili bir modül ya da komut göndermektense, kara listeye alınan makineler/botlar zararlı kodun tüm kötü amaçlı faaliyeti durdurarak uyku moduna geçtiğini görür.

Benzer kendini koruma mekanizmaları elle uygulanmak istendiklerinde, zararlı yazılımın mevcut yeteneklerini geliştirmek üzere Emotet operatörlerinin olağanüstü kaynak yatırımı yapmalarını gerektireceğinden oldukça karmaşık ve pahalı olurlardı. Bu da ESET araştırmacılarını, genel makine öğrenimi algoritmaları kullanılarak çok daha kısa sürede, çok daha ucuz bir şekilde benzer sonuçların elde edilebileceği sonucuna götürmektedir.

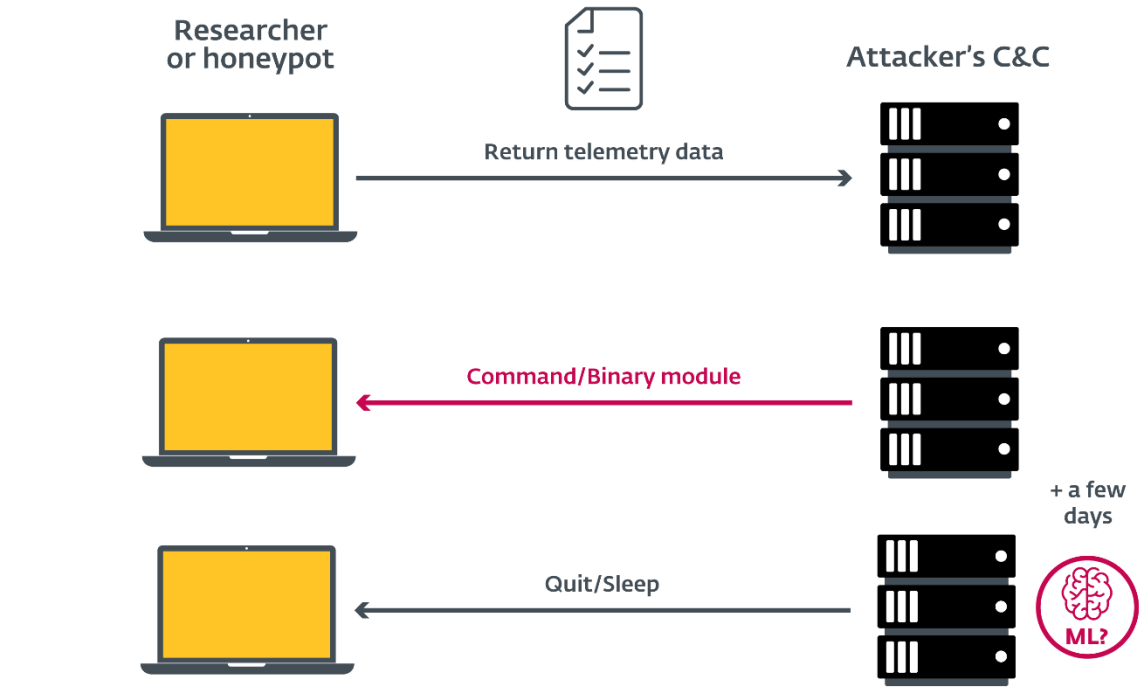
Bir Emotet saldırısının nasıl ortaya çıktığına dair detaylı bir gösterim için aşağıdaki grafiği inceleyebilirsiniz:



Şekil 11: Ele geçirilen kurbanın makinesi, saldırganın C&C sunucusuna özgün telemetrik verileri iletiyor ve komut ya da ikili modül elde ediyor.



Şekil 12: Araştırmacı makinesi (honeypot) yapay telemetrik verileri saldırganın C&C sunucusuna iletiyor ve uyku moduna geç/çıkış yap komutlarını elde ediyor.



Şekil 13: Araştırmacı makinesi iyileştirilmiş yapay telemetri verilerini saldırganın C&C sunucusuna iletiyor, komut ve ikili modül elde ediyor. Emotet birkaç gün sonra tekrar çıkış yap/uyku moduna geç komutuna geçiyor.

Hem spam üretiminde hem de Emotet örneklerinde belirtmek gerekirse, ESET bu gelişmeleri savunma teknolojileri sayesinde ML tabanlı sistemlerin **ağırlıklı göstergesi olarak** tespit etmiştir. Yine de, zararlı

yazılım altyapısı görüntülenemeden uzmanlar için bunu gerçek olarak doğrulamanın bir yolu yoktur. Bu vakalar açıklayıcı nitelikte oldukları için seçildiler; bu belgede belirtilmemiş diğer birçok kötü amaçlı yazılım ailesi benzer otomasyon/ML tabanlı şemalar kullanıyor olabilir.

MAKİNE ÖĞRENİMİNİN SINIRLARI

ESET olarak, ürünün 90'lı yıllardaki ilk sürümlerinden beri çeşitli makine öğrenimi şekilleri üzerinde çalışmaktayız. Bu süreç zarfında uzmanlarımız bu teknolojinin sınırlarını öğrenmeye başladılar:

SINIR #1: DENEME SETİ

Makine öğrenimini siber güvenlik amaçları doğrultusunda etkili bir biçimde kullanabilmek için kötü amaçlı, temiz ve potansiyel olarak güvenli olmayan/istenmeyen uygulamalar (PUSA/PUA) olarak üç kategoriye ayrılmış, yüksek sayıda etiketlenmiş girdi örneği gereklidir.

ESET'in eğitim kaynağı, 30 yılı aşkın bir süredir toplanan milyonlarca örnek arasından dikkatle seçilmiş bir alt gruptur. Bununla birlikte, bir algoritma büyük miktarda veriyle beslenmiş olsa bile, tüm yeni öğeleri doğru bir şekilde tanımlayabileceğine dair bir garanti yoktur. Böylece, insan uzmanlığı ve doğrulamanın sürekli gerekliliği ortaya çıkmaktadır.

Bu süreç olmadan, tek bir yanış girdi bile "kartopu etkisine" yol açarak çözümü başarısızlığa sürükleyebilir. Aynı durum, algoritma ileri öğrenim için girdi olarak yalnızca kendi çıktılarını kullandığında da ortaya çıkar. Hatalar güçlenerek artar; çünkü aynı hatalı sonuçlar çözümü bir döngü içerisine sokarak daha fazla false positive ("FPs": temiz örnekleri zararlı gibi görüp yanlış sınıflandırma) ve false negative (zararlı örnekleri zararsız olarak işaretleme) "çöp" yaratırlar.

SINIR #2: MATEMATİK HER ŞEYİ ÇÖZEMEZ

Bazı gelişmekte olan güvenlik üreticileri, makine öğrenimi tabanlı çözümlerinin yürütme öncesi aşamadaki her örneği analiz edebileceğini öne sürerek bu örneklerin sadece “matematik yoluyla” her zaman temiz (iyi huylu) veya kötü amaçlı olup olmadıklarını belirleyebileceklerini iddia etmekteler.

Ancak bu durumun matematiksel olarak mümkün olmadığı, İkinci Dünya Savaşı sırasında Enigma kodunu kıran İngiliz matematikçi, kriptanalist ve bilgisayar mühendisi Alan Turing tarafından kanıtlanmıştır. Mükemmel bir makine bile gelecekte bilinmeyen bir girdinin istenmeyen bir davranışa sebep olup olamayacağına karar veremez. Genel duruma dair*Durdurma sorunu* olarak da bilinen kanıtı, siber güvenlik de dahil olmak üzere pek çok farklı alana uygulanabilmektedir.

Bu nedenle, bir güvenlik üreticisi çözümünün her numuneyi düzgün bir şekilde çalıştırmadan temiz veya kötü amaçlı olarak etiketleyebileceğini iddia ediyorsa, dikkatli olun. Bunu başarmanın bir yolu, karar verilemeyen öğelerin büyük bir kısmını önceden engellemek ve BT güvenlik departmanınızın yanlış tespitlerle boğuşmasını önlemektir. Diğer bir seçenekse daha az hatalı tespite sahip, daha pasif bir tespit olmakla birlikte, yalnızca makine öğrenimi kullanarak tespit oranlarının iddia edilenin aksine "%100" seviyesinden çok daha uzak bir verimlilikle belirlenmesine dayanmaktadır.

SINIR #3: AKILLI VE UYARLANABİLİR DÜŞMAN

Siber güvenlikte makine öğrenimi uygulamalarındaki bir diğer ciddi sınırlama ise **akıllı düşmandır**. Elbette makineler Go ve satrançta insanları yenecek kadar akıllı duruma gelmiştir; ancak bu oyunların bağlayıcı kuralları vardır. Konu siber güvenlik olduğunda saldırganlar genellikle hiçbir uyarı olmadan tüm oyun alanını değiştirerek hiçbir kuralı çiğnemek için tereddüt etmezler.

Dijital ortamın sürekli değişen yapısı, gelecekteki tüm tehditleri algılayabilen ve engelleyebilen koruyucu bir çözüm oluşturmayı imkansız kılmaktadır. Ve makine öğrenimi bu varsayımı değiştirmiyor.

SINIR #4: YANLIŞ TESPİTLER (FALSE POSİTİVES)

Zararlı yazılımın tespit edilememesi bir kuruluş için anlaşılabilir bir endişe kaynağı olsa da, temiz öğelerin hatalı bir şekilde zararlı olarak etiketlendiği yanlış tespitlerde (FP) bu durum daha az anlaşılabilir haldedir.

Her yanlış tespit tüm BT altyapısını tam anlamıyla çöküşe sürüklemese de, bazı kuruluşlar için FP pek çok zararlı yazılımdan daha büyük bir potansiyel yıkıcı güce sahiptir. Eğer FP güvenlik yazılımının üretim hattında kullanılan yazılımı engellemesine ya da kaldırmasına neden olursa, üretim kesintiye uğrayacaktır. Böyle bir senaryo büyük aksaklıklara ve milyonlarca dolarlık maddi zararla birlikte belki de itibar kaybına neden olabililir.

Yanlış tespitler, üretim yapmayan kuruluşlarda BT güvenlik çalışanlarının kapasitelerini zorlayabilir, hatta siber güvenlik konumlarında hatalı ayarlamalar yapmalarına neden olabilir ve bu doğrultuda çok daha büyük maliyetlere sebep olabilirler.

SINIR #5: MAKİNE ÖĞRENİMİ TEK BAŞINA YETERLİ DEĞİLDİR

Bazı yeni siber güvenlik üreticileri, makine öğrenimi teknolojisini siber güvenlikle ilgili tüm sorunları çözen sihirli bir çözüm olarak sunmaktadır. Bu alanda 30 yıl, makine öğrenimi konusundaysa 20 yılı aşkın sürede edindiğimiz tecrübeler doğrultusunda ESET uzmanları, en yeni makine öğrenimi algoritması olsa bile yalnızca tek bir teknolojiye dayanan bir güvenlik yaklaşımının tehlikelerini bilirler.

Yalnızca makine öğrenimi ve insan uzmanlığı da dahil olmak üzere birden fazla güvenlik katmanının incelikle harmanlanmış bir karışımı, düşük sayıda yanlış tespit ile birlikte en yüksek algılama oranlarını sunabilir.

KÖTÜ AMAÇLI ML'NİN BİLE SINIRLARI VARDIR

Diğer herhangi bir alanda olduğu gibi, ML'nin zararlı yazılımlara ve kötü amaçlı faaliyetlere uygulanmasının da bezi **sınırları** vardır. Bunların belki de en önemlisi, yaygın şekilde kullanılarak belgelenmiş ilk siber silah olan Stuxnet'tir.

Bu zararlı yazılım, korunan ve hatta hava boşluğu bulunan herhangi bir ortamı ele geçirerek hedeflenen sistemin de ötesine yayılabilmesiyle oldukça etkili olmuştu. Bu saldırgan tutum güvenlik araştırmacılarının dikkatini çekti ve onlar da nihai olarak bu tehditi tespit ederek incelediler.

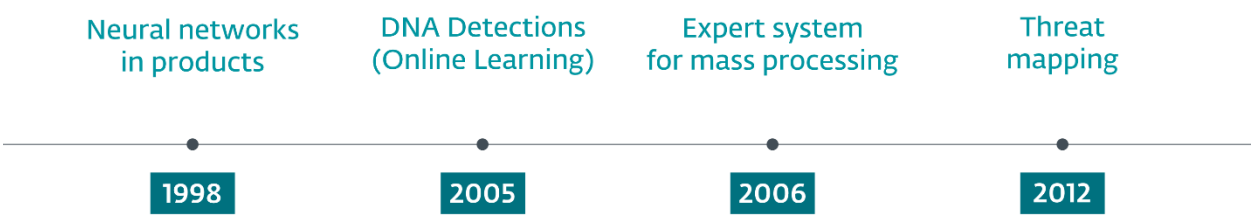
Benzer durumlar gelecekte meydana gelecek pek çok ML destekli saldırıda da yaşanabilir. Sızıntıların sayısı arttıkça, tehditler daha yaygın hale gelerek savunucuların tarafında daha fazla dikkat çekecektir. Bu da nihai olarak tespit edilip hafifletilmelerine neden olacaktır.

ESET VE 20 YILLIK MAKİNE ÖĞRENİMİ

Siber güvenlik çok daha derin köklere dayansa da, makine öğrenimi yeni ortaya çıkan güvenlik üreticilerinin geçtiğimiz birkaç yıl içerisinde konuşmak istediği tek konu gibi görünüyor. Ortaya çıkış tarihi 1950'lere uzanmakla birlikte, teknik ve performans anlamındaki pek çok sınırlamaya rağmen, 2000

yılından önce bile güvenlik ürünlerinin gerçek dünya uygulamalarında kullanılmıştır ve bunlardan biri de ESET'in algılama motorudur.

Uzmanlarımız makine öğreniminin potansiyelinin farkına vararak sinirsel ağların kullanılması yoluyla tespitlerimizin geliştirilebilmesi için 1998 yılından beri onları ESET ürünlerinin bir parçası haline getirmiştir.



Şekil 14: ESET'in makine öğrenimi kullanım çizelgesi

ESET 2015 yılında DNA Algılama olarak adlandırılan yeni bir makine öğrenimi tabanlı teknolojiyi duyurdu. Bu teknoloji, analiz edilen dosyayı eşleştirme ve algılama için daha uygun bir forma dönüştürüp özellikleri; yani "genleri" belirli şekilde seçerek bir DNA tespit mekanizması inşa eder.

Bu DNA algılamaları, aradaki boşluğu zararlı ve temiz ikili sistemler şeklinde bölerek karışık modelleri karakterize etmektedir. İster gerçek araştırmacılar, ister otomatize edilmiş sistemler tarafından oluşturulmuş olsun; düzenli olarak güncellenen bu model 2005 yılından beri "çevrimiçi makine öğrenimi modelimiz" olarak hizmet vermektedir.

DNA Algılamalarının bilinen ve önceden görülmemiş tehditlere karşı etkinliğinden esinlenerek makine öğrenimine odaklanmış bir dizi dahili proje ortaya çıkmış, bunlar arasında günde yüz binlerce örneği işleyen gelişmiş backend sistemlerinin yanı sıra, araştırmacılara tehdit haritası çıkarma imkanı tanıyan ML tabanlı yeni araçlar yayınlanması da yer almıştır.

Ardından 2010'lara gelindiğinde bir değişim ivmelenmeye başlayarak bu teknolojinin önünde yeni fırsatlar oluşmasını sağlamıştır.

Büyük veri ve ucuz donanım, makine öğrenimini siber güvenlik tehditlerinin tespit edilmesinde olduğu kadar, sağlık sektörü ve otonom araçlar gibi çeşitli alanlarda da uygulanabilir ve ulaşılabilir kılacak veri ve altyapı olanaklarını sağlamıştır.

Makine öğrenimi algoritmalarının artan popülaritesi, ML alanında artan bir yatırıma yol açarak akademik konulardan pratik araştırmalara dek pek çok alanda ML uygulanabilirliğine katkıda bulunan yeni gelişmelerin önünü açmıştır.

Bu noktada ESET, yıllardır sürdürdüğü araştırma ve geliştirme faaliyetlerini kullanmaya hazırdı ve bu doğrultuda makine öğrenimine dayalı yeni, son derece sağlam bir tespit motoru oluşturmaya başladı. Siyah şapkalılarla savaşılan otuz yılın ardından uzmanlarımız günümüzün zararlı yazılımlara yönelik "İskenderiye Kütüphanesi" denilebilecek bir yapı kurdular. Bu geniş ve son derece organize koleksiyon, elde edilen milyonlarca özellik ve DNA geni yoluyla makine öğrenimi motorumuzu**eğitmek üzere yüksek kaliteli malzeme sunar**,

Ancak ML ile ilişkili alanlardaki bu patlama yeni zorlukları da beraberinde getirmiştir. ESET uzmanları, en iyi performans gösteren yaklaşımları ve algoritmaları kapsamlı bir şekilde test etmek ve elle seçmek zorunda kaldılar; çünkü hepsi bu son derece özel güvenlik ortamına eşit derecede uygun değildi. Son aşamada, ESET iki metodolojinin bir karışımında karar kıldı:

- **Çeşitli derin öğrenme yöntemleriyle işleme**
- **Çoklu model işleme (denetimli öğrenim yöntemlerinin birleştirilmesi)**

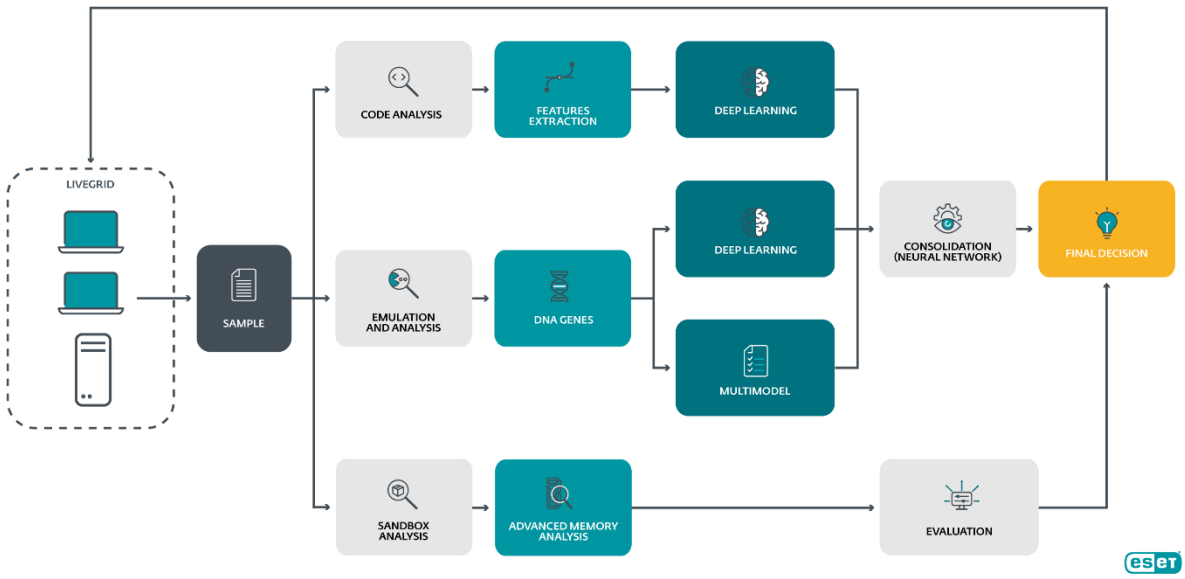
ESET'in sınıflandırma algoritmaları ve derin öğrenim yöntemleri de dahil olmak üzere dizayn ediliş biçimi, yalnızca algılama motorunun isabet oranını artırmakla kalmaz; aynı zamanda düşmanca etkinliğe karşı dayanıklılığa da katkıda bulunur. 2018'de yayınlanan bir makalede belirtildiği gibi[2]; benzer yapıya sahip makine öğrenimi tabanlı bir sistemi, toplanan örneklerin yanlış sınıflandırmasını zorlayan hataya dayalı bir saldırı üzerinden ESET'in ML algoritmasına karşı başarılı olmak için saldırganın tarafında çok daha karmaşık bir strateji gerektirecektir.

ESET, ML SÜREÇLERİNİ NASIL ÖRNEKLENDİRİYOR (ŞEKİL15)

ESET ML motoruna girdikten sonra her örnek:

1. Özelliklerinin tespit edildiği statik kod analizine tabi tutulur ve derin öğrenme algoritmalarıyla işlenen veri toplanır
2. Dinamik analizin bir parçası olarak emüle edilir ve bir dizi DNA geni üretir. Bunlar, dikkatle seçilmiş sınıflandırma modelleri ve başka bir derin öğrenme algoritmasıyla beslenir.
3. Aynı zamanda, bu örnek bir sanal ortamda yürütülür ve gelişmiş bellek analizine tabi tutulur. Çıktı; bilinen, düzenli olarak gözden geçirilen ve otomatik olarak güncellenen temiz ve kötü amaçlı öğe kümesiyle karşılaştırılmak üzere yerel-duyarlı hash işlemi için kullanılır.
4. Önceki adımlardan elde edilen sonuçlar, bir sinir ağı veya diğer değerlendirme biçimleri aracılığıyla vektör haline getirilerek konsolide edilir.
5. Toplanan tüm bilgiler doğrultusunda örneğin temiz, potansiyel olarak istenmeyen veya kötü niyetli olduğu belirlenecek şekilde nihai bir karar oluşturulur.
6. Bu bilgi daha sonra ESET LiveGrid® aracılığıyla ESET kullanıcılarına iletilir.

[2] Battista Biggioa, Fabio Rolia, Wild Patterns: Düşman Makine Öğreniminin Yükselişinden On Yıl Sonra, (2018), 6-7



Şekil15: ESET ML ile örneklerin nasıl işlendiğini detaylandıran şema

ESET'in bazı yeni ortaya çıkan güvenlik üreticilerinin aksine, örnek işleme sürecinin bir parçası olarak emülasyonun yanı sıra paket açma ve davranış analizinden de yararlandığını belirtmek önemlidir. Bu adımlar, bir örnek ML motoruna iletilmeden önce sahip olduğu özelliklerin düzgün bir şekilde belirlenebilmesi açısından kritik önem taşımaktadır. Sıkıştırılmış veya şifrelenmiş örnekleri analiz etmek, alakasız sonuçlar doğuracak gereksiz bilgileri sınıflandırmaya yönelik bir girişimle eşdeğerdir. Bu yaklaşım, bir şarkı yarışmasında sadece adayların fotoğraflarına bakarak, onlara performans gösterme şansı vermeden yarışmanın kazananını seçmek gibidir.

MEVCUT ESET ÜRÜNLERİNDE MAKİNE ÖĞRENİMİ

ESET Makine Öğrenimi'nin gücü, her boyuttaki müşteriler tarafından erişilebilirdir. ESET LiveGrid® özelliğine sahip her uç nokta ve cihaz, bu son teknoloji ESET ML motorunun doğru tespit ve olası tehditleri analiz etme yeteneğinden yararlanır.

ESET'in büyük ölçekli kurumsal müşterileri, ayrıca üç üst düzey ürün aracılığıyla makine öğrenimi teknolojisini kullanabilmektedir:

1. **ESET Enterprise Inspector (EEI)**
    - EEI, ESET'in Uç Nokta Algılama ve Tepki (EDR) aracıdır. Uç noktada devam eden faaliyetlere ilişkin gerçek zamanlı veriler toplayarak çalışır ve bu veriler daha sonra şüpheli faaliyetleri otomatik olarak tespit edebilmek üzere bir dizi kuralla eşleştirilir. Toplanan bilgiler işlenir, kümeler halinde toplanır ve aranabilir biçimlerde saklanır; böylece sıradışı ve şüpheli faaliyetlerin ayrıntılı bir özeti oluşturulur.
    - EEI ayrıca kurumsal güvenlik ekibine geçmiş olayların adli olarak soruşturulması konusunda bilgi sağlayarak ağdaki tehdit aktörlerinin (gelişmiş kalıcı tehdit veya APT) varlığını hafifletmek için tepkisel yetenekler sunar. EEI, makine öğrenimi de dahil olmak üzere ESET algılama teknolojileri tarafından sağlanan şüpheli faaliyetler ve örnekler hakkındaki bilgilerden yararlanır.

2. **ESET Dynamic Threat Defense (EDTD)**
    - EDTD, daha önce görülmemiş yeni tehdit türlerini algılamak üzere bulut tabanlı sandbox teknolojisi kullanır ve böylece Mail Security ve Endpoint ürünleri gibi ESET ürünlerine ek bir güvenlik katmanı sağlar. Bu sandbox; kodun statik analizini, örneğin makine öğrenimi ile derinlemesine incelemesini, bellek içi dahili gözlem ve davranış tabanlı algılamayı tamamlayan çok sayıda farklı tipteki sensörden oluşur. Endpoint ile karşılaştırıldığında EDTD, son 30 yılda ESET tarafından toplanan geniş kapsamlı temiz, istenmeyen ve kötü amaçlı öğelerin bulunduğu veri havuzuna erişim sağlayan çok daha güçlü bir algılama motorunu temsil eder. Böyle bir çözümü bulutta çalıştırmak çok daha etkilidir; böylece çözüm daha ölçeklenebilir hale getirilerek müşterinin altyapısına yönelik talepler azaltılmış olur.
3. **ESET Threat Intelligence (ETI)**
    - ESET Threat Intelligence, mevcut veya yeni ortaya çıkan tehditlerle ilgili kanıta dayalı bilgiler sunar. ETI, belirli bir müşteriye yönelik küresel siber alandaki kötü amaçlı yazılımlar veya etkinlikler hakkında erken uyarı imkanı sağlayabilir. ESET makine öğrenimi ve diğer algılama teknolojileri tarafından sağlanan bu bilgiler, BT güvenlik departmanlarındaki veya güvenlik operasyon merkezlerindeki (SOC) analistler için uygun, insanlar tarafından okunabilecek bir biçimde analiz edilerek sunulur.
    - ETI müşterilere çıktı olarak sunulan ayrıntılı bir raporla birlikte, makine öğrenimi de dahil olmak üzere ESET'in algılama motoru aracılığıyla analiz için seçilen örnekleri gönderme imkanı da sunar.

Makine öğreniminin tam potansiyeli henüz ortaya çıkmamış olsa da, mühendislerimiz sürekli olarak ESET portföyünde bu teknolojinin kullanımından yararlanabilecek görev ve ürünleri aramaktadırlar.

SONUÇ

Makine öğreniminin hangi etkilerinin olumlu ya da olumsuz olacağını söylemek zor olsa da, siber güvenlik bölünmesinin her iki tarafında da ML destekli sistemlerin giderek artan kullanımı sonucu tüm internet güvenliğininin geri dönülemez bir şekilde dönüşüme uğradığı bir gerçektir.

ESET, araştırmalara dayalı tahminlerimizin yanı sıra, istenmeyen posta ve Emotet örnekleriyle görsellleştirilen teknolojik gelişmelerin işaretleriyle siyah şapka dünyasındaki gelişmeleri yakından izlemekte ve koruyucu çözümlerini sürekli geliştirerek tepki vermektedir.

Ancak, gelişmekte olan birçok siber güvenlik oyuncusunun pazarlama kampanyalarına rağmen, ESET'in otuz yıllık deneyimi, makine öğrenimi veya derin öğrenme de olsa, yalnızca tek bir teknolojiye güvenilerek gerçek korumanın sağlanamayacağını göstermektedir.

Her ölçekteki kuruluşların sahip oldukları güvenlik çözümünün saldırılara karşı dayanıklı olmakla birlikte yüksek tespit oranlarına ve düşük yanlış tespit sayısına sahip olabilmesi için çok katmanlı bir yaklaşım benimsemesi gerekmektedir.

YÖNETİCİ ÖZETİ

Makine öğrenimi alanındaki gelişmeler tamamen yeni bir çağ başlattı. Siber güvenlik de dahil olmak üzere, toplanan neredeyse her veri parçasının makine öğrenimi teknolojisine bağlı algoritmalar aracılığıyla işlenip analiz edildiği bir dönem... Yine de bu yeniliğin bile bazı dezavantajları ve sınırlamaları bulunmaktadır.

Bu doküman, makine öğrenimi teknolojisinin çeşitli alanlarda neden olduğu hareketliliği ve kurumsal karar vericileri nasıl etkilediğini açıklamayı amaçlamaktadır.

Ayrıca ESET araştırması tarafından gözlemlenen, ML kullanımının güçlü göstergelerine sahip olan, yerel spamlardaki iyileştirmeler ve Emotet kötü amaçlı yazılım saldırıları gibi aktif siber saldırıları da özetliyoruz.

Son olarak, ESET'in makine öğrenimi konusundaki 20 yıllık tecrübesinin görüşlerimizi nasıl şekillendirdiğini, arka plandaki eski uygulamalara olduğu kadar, ESET'in güncel ürünleriyle daha iyi görülebilecek şekilde ortaya koyuyoruz.