Kısa bir zaman içinde ortaya çıkan bu unsurlar, gelişmiş sürekli tehdit (APT) gruplarının ve siber suçluların düzenlediği süregelen ve gelişen tehditler karşısında sistemin sağlamlığını korumanın zorluğunu artırıyor. Yasalara uygun hareket etme ve kısıtlı bütçelerle hareket etmek zorunda olma, bilgi güvenliği yöneticilerinin uykularını kaçırıyor.

Koronavirüs kısıtlamaları ve buna bağlı olarak çalışanların, şirket verilerinin ve kurumsal verilerin yanı sıra BT altyapısına artan bir şekilde evden erişim sağlaması siber suç çetelerinin ve devlet aktörlerinin iştahını kabartıyor. Aslında her iki grup da amaçlarına ulaşmak üzere bu çalkantılı zamanı kendi yararına kullanarak giderek artan bir yoğunlukta saldırılar düzenliyor. Örneğin, pandemi sırasında özellikle RDP saldırısı girişimleri, 2020 yılının birinci çeyreği ve dördüncü çeyreği arasında %768 oranında *arttı*.

"Kanada Hükümetinin" *temaslı izleme uygulaması* gibi hizmetler dahil olmak üzere özellikle bir hükümet hizmetini taklit eden, COVID-19 gibi gündemdeki konularla ilgili tehditler de ESET tarafından tespit edildi. COVID-19 kısıtlamaları süresince, *"resmi Kolombiya Hükümeti" e-posta yazışmalarıyla kimlik avı* amacıyla istikrarlı saldırılar, *OceanLotus tarafından* Güneydoğu Asya hükümetlerine su kaynağı saldırıları ve buna benzer birçok saldırı hükümet ile saldırının hedefindeki vatandaşları karşı karşıya getiriyor.

COVID-19'un sağlık alanındaki etkilerini azaltma konusunda mücadele veren hükümetler, vatandaşlara hizmet vermelerini etkileyen siber saldırıların, veri hırsızlığının veya stratejik ulusal altyapı ihlallerin arttığını belirtiyor. Son zamanlarda görülen başlıca saldırılar arasında *SolarWinds Orion bilgisayar saldırısı*, *Microsoft Exchange ihlali* ve *Centreon* BT altyapı izleme aracına yönelik saldırılar yer alır. Bu saldırılar, Fransa'daki ve Almanya'daki sağlık hizmetleri sistemlerini kasti olarak hedef alır. Ayrıca okullardaki, üniversitelerdeki platformlara ve eğitimle ilgili BT platformlarına saldırılar da giderek artıyor.

Verilere ve genel eğilimlere göz attığımızda, APT gruplarının ve siber suçluların taktiklerini geliştirmeye devam ettiklerini ve COVID-19 ile ilgili endişelerden yararlanarak, yaygın kullanılan uygulamaları daha fazla hedef almaya başladığını görüyoruz.

Örneğin, 2020 yılının başlarında XDSpy APT grubu operatörleri *bir e-posta oluşturdu.* Bu e-posta, Belarus'taki ilk koronavirüs vakalarını onaylamak üzere Belarus otoritelerinden gelmiş gibi görünüyordu. Ancak bu e-postalar sosyal medya ağlarında yanlış bilgilerin dolaşmasına neden olmanın yanı sıra kötü amaçlı yazılıma yönlendiren bir bağlantı da içeriyordu.

Siber Casusluk

Geleneksel anlamda hükümet kurumlarının düşmanlarının, politik ve ekonomik çıkarlarını korumak üzere hassas verileri çalmaya çalışan ve gittikçe artan bir şekilde sorun yaratan, zarar veren ve aksamalara neden olan devlet aktörleri olduğu düşünülüyor. Devletler arasındaki bu rekabet düzenli olarak gri bölgede gerçekleşir, bu sayede gerçekçi inkara dayalı olarak birbirleriyle ilişki kurabilirler. Günümüzde yaygın olarak görülen bu siber spor dahilinde, sürekli olarak yüksek önceliğe sahip bir hedef olan ekonomik alanda, *aşı geliştirenlerin* ve bu kuruluşların tedarik zincirlerinin hedef alınması da dahil fikri mülkiyet hakkının çalınmasına dair çabalarda büyük bir artış görüyoruz. Bu etkinlikler, aksi bir durumla karşılaşmadıkları sürece, hükümetlerin vatandaşlarını korumasını ve vatandaşlarına hizmet sağlamasını sekteye uğratır.

Veri çalmaya çalışan veya gerçek dünyada olanları etkilemeye uğraşan saldırganlar dolayısıyla ulusal düzeyden yerel düzeye kadar çeşitli kamu sektörleri; suç gruplarının veya bilgisayar korsanlarının yanı sıra bu devlet aktörlerine karşı tutumlarını değiştirmelidir. Devlet aktörü etkinliği giderek artarken bu aktörlerin hedefinde olmayacağını düşünen bazı kurumlar olabilir. Ancak kurumların birbirine bir şekilde bağlı olduğunu düşünürsek, dünya genelinde devletlerin birbirleriyle rekabet ettikleri bir alandaki etkinlik, farkında olmadan bu bağlamla ilgisi olmayan ülkeleri ve kuruluşları etkileyebilir. Siber alandaki bu gittikçe büyüyen savaşta dolaylı olarak zarar görmek gerçek bir risktir.

Günümüzde oldukça cesur bir şekilde hareket eden ve gizlenmeye gerek duymayan APT gruplarından biri de *Gamaredon*'dur. Bu grubun çalışma tarzı, örneğin Ukrayna'nın çeşitli kurumlarındaki bireyleri hedef almak üzere Microsoft Word ve Excel gibi popüler uygulamaları hedefleyen şablon enjeksiyon kullanımını ve neredeyse her yerde bulunan Microsoft Outlook'taki toplu posta makrolarını içerir.

Gamaredon, hükümette ve şirketlerde kullanılan yasal araçları hedeflediğinden, bir makinenin parmak izini alma ve hangi hassas verilerin bulunduğunu anlayıp ağa yayılma konusunda oldukça etkili olabilir. Geçtiğimiz günlerde grubun özel olarak geliştirilmiş bir kötü amaçlı yazılıma geçtiğini belgeledik.

Tespit edilmeyi engellemek üzere, özel bir açık kaynak PowerShell yükleyici gibi dosyasız bir kötü amaçlı yazılım veya bugünlerde yoğun olarak hedef alınan Microsoft Exchange sunucularına zarar vermek üzere özel olarak oluşturulan *LightNeuron* kötü amaçlı yazılımı gibi etkileyici araçlara sahip Turla APT grubu, özellikle hükümet kurumları veya savunma şirketleri gibi yüksek profile sahip hedefler seçiyor. Kazandığı şöhretine ek olarak Turla, 2020 yılının son çeyreğinde belgelediğimiz *Crutch*'ın yeni bir sürümünü oluşturdu. Bu kötü amaçlı yazılım, harici sürücüleri izliyor, komuta ve kontrol iletişimi için bulut depolamayı suistimal ediyor.

Fidye yazılım: İnovasyon ve sürekli baskı

Yapısı gereği suça yatkın olan APT grupları ile devletlerin desteklediği aktörlerin bir arada bulunduğu bir ortamda, hedefe yönelik fidye yazılımların hükümet kurumları ve ilişkili şirketler için gittikçe büyüyen bir endişenin işaretçisi olduğunu söyleyebiliriz. Ayrıca, çeşitli suç gruplarının verilere erişim sağlamak, verileri çalmak veya şifrelemek, ödeme almak veya para aklamak için bir arada çalışması da endişe uyandıran bir konudur.

2020 yılının Ekim ayında ESET'in Microsoft, NTT Ltd. ve birçok emniyet kuruluşuyla Trickbot botnetleri çökertmek amacıyla işbirliği yapması sonucunda, operatörlerin Trickbot ile hesaplardan para çalmaktan tüm şirkete sızmaya geçiş yaptığı birçok karmaşık etkinlik ortaya çıktı. Bu operatörler etkilenen sistemlerin tekrar kullanıma açılması için fidye talep etmek üzere Ryuk'u yürütmek üzere Trickbot'u kullanıyordu. Trickbot etkinliği azalırken *ESET telemetrisindeki algılamaların artması* da ilginç bir durumdur. Trickbot indirmek dahil olmak üzere Emotet botnet etkinlikleri büyük bir artış gösterdi.

Ortaya çıkan bağlantı sayesinde, nihayetinde 2021 Ocak ayında en uzun ömürlü ve en yaygın kötü amaçlı yazılım tehditlerinden biri olan *Emotet çökertildi.* Europol tarafından yürütülen geniş çaplı bu çökertme operasyonunda, Avrupa'dan ve Kuzey Amerika'dan çok sayıda ulusal emniyet kuruluşu yer aldı.

Risklerin bu kadar yüksek olduğu bir durumda servis boyutlandırmasını ve iç süreçleri savunmakla görevli güvenlik personeli, devlet aktörlerine karşı uyanık olmak ve APT gruplarının sürekli değişen taktikleri, teknikleri ve prosedürleri ile başa çıkmak arasında sıkışıp kalıyor. Ayrıca net ürün ve hizmet teklifleri sunan bu organize suç sektörünün ortaya çıkması, saldırganlar arasındaki inovasyonu ve inisiyatifi gösteriyor. Bu gruplar, en yüksek ödemeyi elde etmek için potansiyel kurbanları değerlendirmenin ötesine geçerek, verilerin satışını en yüksek düzeye çıkarmak üzere günümüzde iyi yapılandırılmış suç piyasası platformlarına dönüşüyor.

Ayrıca bu gruplar hedefledikleri sistemlerde haftalarca veya aylarca kalarak sistemi keşfediyor, veri topluyor ve *son olarak sisteme fidye yazılım yerleştiriyor*. Bazı gruplar için bu durum yüksek miktarda para kazanmak anlamına gelirken, bazı grupların amacı sızdıkları hükümete ve bu hükümetin sunduğu hizmetlere zarar vermektir. *Birçok hükümet fidye ödemediğini açıkça belirtse de* kurban durumuna düşebilir. Hükümetlerin dikkatini dağıtabilecek ve yoğun bir şekilde kaynak ayırmasını gerektirecek "yaylım ateşi" taktiği gibi yöntemlerle başarı sağlandığı takdirde bu durum hükümetler için fidye kadar zarar verici olabilir.

Tedarik zinciri saldırıları hızlı bir şekilde artıyor

Kazara veya kasti olarak tedarik zincirinin çökertilmesi ilk çağlardan bu yana görüldüğünden tedarik zincirinin güvenliği ve sağlamlığı artırılmalıdır. Ancak, üçüncü taraf sağlayıcıların sağladığı dijitalleşme ve işbirliği yararları, *tedarik zincirine yönelik saldırı riskinin artmasına da neden oluyor.*

2017 yılındaki *DiskCoder.C* (NotPetya olarak da bilinir) saldırısı bunun en iyi örneklerindendir. Bu olayda, birçok şirket ve iş ortağı tarafından tedarik zincirinin bir parçası olarak kullanılan ve bölgesel olarak oldukça popüler olan M.E.Doc muhasebe yazılımı, kullanıcıların şirketlerinin çökertmek üzere bir silaha dönüştürüldü. Öngörülmüş olsa da, olmasa da, dünya genelinde tedarik zincirinin bir parçası olarak lojistik hizmeti veren birçok küresel şirket de bu olaydan dolaylı olarak etkilendi.

Hızla geçen üç yılın ardından, şirketler açısından tehlike arz eden muhasebe yazılımları yerine bu kez *SolarWinds Orion saldırısında oldukça büyük bir sürekli kampanyayla karşılaştık.* Bu platformdaki binlerce kullanıcıyı etkileyen saldırı, yaygın suç ve APT gruplarının etkinlikleri için potansiyel oluşturdu.

ESET araştırmacıları geçtiğimiz aylarda başka tedarik zinciri saldırılarını da ortaya çıkardı. Bunlar arasında ele geçirilmiş güvenlik eklentilerini kullanan *Lazarus gruptan* şirketlerin kullandığı bölgeye özgü sohbet yazılımına saldıran *Stealthy Trident Operasyonuna*, hükümet sertifika otoritesini ihlal etmek için kullanılan *SignSight Operasyonundan* bilgisayar korsanlarının ele geçirdiği Android emülatörü *NightScout Operasyonuna* kadar birçok saldırı yer alır.

Yeni normal çalışma yeri; ev

Evden ve hibrit çalışma, tüm çalışanlar ve dolayısıyla hükümet kurumları için riskleri önemli ölçüde artırıyor. COVID-19 sonrasında da mevcut hibrit çalışma modeli bir şekilde devam edeceğinden, bu düzenlemeler kalıcı olacak ve riskler devam edecektir. Sistem güvenliği açısından bakıldığında ev ortamı, harekete geçmeye hazır ve gittikçe karmaşık hale gelen siber çetelerin siber saldırılarına açık "çiftlik evleri" ve "mevzi noktaları" ile dolu Vahşi Batı'yı andıran bir yerdir.

Siber güvenlik ihlallerinin %23'ünün insan hatasından kaynaklandığı belirtiliyor. Saldırganlar genellikle, yasal gibi görünen bağlantılara tıklanmasını (milisaniyeler içerisinde) sağlayan insani içgüdülerden yararlanır. Ancak en büyük ihlallerin bazıları, deneyimli BT profesyonellerinin eylemlerinin sonucunda gerçekleşir. Bu kişiler daha fazla bilgi sahibidir, ancak kişilerin kendi cihazlarıyla bağlanması, bulut sisteminin yanlış yapılandırılması veya diğer yanlış uygulamalar sonucunda ihlaller gerçekleşir. Personel eğitimlerinin artırılması ve süreçlerin güçlendirilmesi, gereken güvenlik davranışlarının kalıcılığı açısından kuşkusuz çok önemlidir.

Bilgisayar korsanlarının saldırılarına karşı çok dikkatli davranılmasına rağmen, *2020 yılı için İçeriden Tehditlerin Maliyeti: Küresel Rapor* adlı Ponemon Institute tarafından yayınlanan rapora göre, içeriden kişilerin neden olduğu olayların sayısı 2018 yılında 3.200 iken %47'lik bir artışla 2020 yılında 4.716'ya çıkmıştır. Bu ihlallerin birçoğunun nedeni insan hatasıdır, ancak içeriden saldırıların bazıları *hoşnutsuz çalışanlardan kaynaklanır.* Bunlar intikam, kişisel çıkar veya daha da ileri gidersek yeni bir çalışana veya bir devlet aktörüne çıkar sağlamak üzere veri hırsızlığını, fiziksel hasarı veya hesapların silinmesini içerir. Özellikle yönetici ayrıcalıklarına sahip çalışanların düzenlendiği bu saldırıları, uç nokta algılama ve tepki aracı veya uzman bir personel tarafından kullanılan gelişmiş tespit çözümleri olmadan algılamak zordur.

Hedef alınsa da yalnız değil

Günümüz dinamik güvenlik ortamında, siber güvenlik özelliklerinize çok fazla güvenmemeniz, gittikçe daha önemli bir hale geliyor. Siber riskler, azalmak yerine artıyor. Düzenli inceleme, testler ve *saldırı senaryosu alıştırmaları,* saldırılardan uzak durmanıza ve saldırıları hızlı bir şekilde kontrol altına almanıza yardımcı olma açısından önemlidir. Devlet tarafından desteklenen aktörlere sağlanan becerilerden ve araçlardan ötürü, hedef olmanın veya dolaylı olarak zarar görmenin doğurduğu risklere karşı korunmak için çok katmanlı karmaşık savunma, aktif izleme, güncel *tehdit istihbaratı* ve her zamankinden çok daha eğitimli bir güvenlik ekibi gerekir.

Sürekli gelişen tehditlere karşı bakış açınızı genişletmek, sisteminizi daha iyi bir şekilde korumanıza yardımcı olmanın yanı sıra paydaşlarınızı, şirketlerinizi ve rehberlik için hükümet kurumlarına güvenen vatandaşları daha iyi bilgilendirmenizi sağlar. Karmaşanın ve üzüntünün hakim olduğu bir yılda, siber güvenlikteki olumlu eğilimlerden biri de koronavirüsle savaşmanın yanı sıra bu zorluklarla mücadele etmek üzere kamu ve özel sektörün güçlü bir ortaklık kurmasıdır. ESET, bu durumdan memnundur ve daha güvenli bir dijital dünya sağlamak üzere hükümet ortaklarıyla birlikte çalışmayı arzular.

2

AVRUPA'DAKİ APT SALDIRILARI: HÜKÜMETLER İÇİN GİDEREK BÜYÜYEN BİR SORUN

Geçtiğimiz altı ay içinde APT gruplarının gerçekleştirdiği saldırılar sıradan saldırılar mıdır yoksa tedarik zinciri saldırılarında yeni ortaya çıkan bir akım mıdır?

Robert Lipovský
Kıdemli Kötü Amaçlı Yazılım Araştırmacısı

Geçtiğimiz altı ay içinde gelişmiş sürekli tehdit (APT) saldırılarında hızlı bir artış oldu. Bu saldırılar, Avrupa kıtasında Fransa'dan Doğru Avrupa'ya ve Balkanlara kadar birçok ülkedeki hükümet ile askeri kuruluşları ve özel şirketleri hedef aldı.

ESET tarafından ortaya çıkarılan APT etkinliklerine bir örnek de *Crutch*'ın yeni sürümüdür. Bu sürüm daha önce belgelenmemiş bir arka kapıdır ve kötü şöhrete sahip Turla APT grubuna ait bir dosya hırsızıdır. ESET araştırmacıları, Crutch'ı bir Avrupa Birliği ülkesinin dış işleri bakanlığının ağında gördü. Ortaya çıkarılan bir diğer etkinlik de *Gamaredon*'dur. Kötü amaçlı bu grup, durmaksızın Ukrayna'daki hükümet kuruluşlarını hedef almasıyla tanınır ve 2020 yılında *kötü amaçlı yazılım cephaneliğini* güncellemiştir.

Aşağıdaki metinde diğer iki örneği yakından inceleyeceğiz: Dokuz yıldır radara yakalanmamayı başaran bir APT grubu olan *XDSpy* ve en tehlikeli APT gruplarından biri olan Sandworm.

Ayrıca, SolarWinds saldırısının uluslararası haberlerde yer almasından bu yana daha fazla dikkat çeken bir konu olan, çeşitli tehdit aktörlerinin cephaneliğinde tedarik zinciri saldırılarının oynadığı rolden bahsedeceğiz.

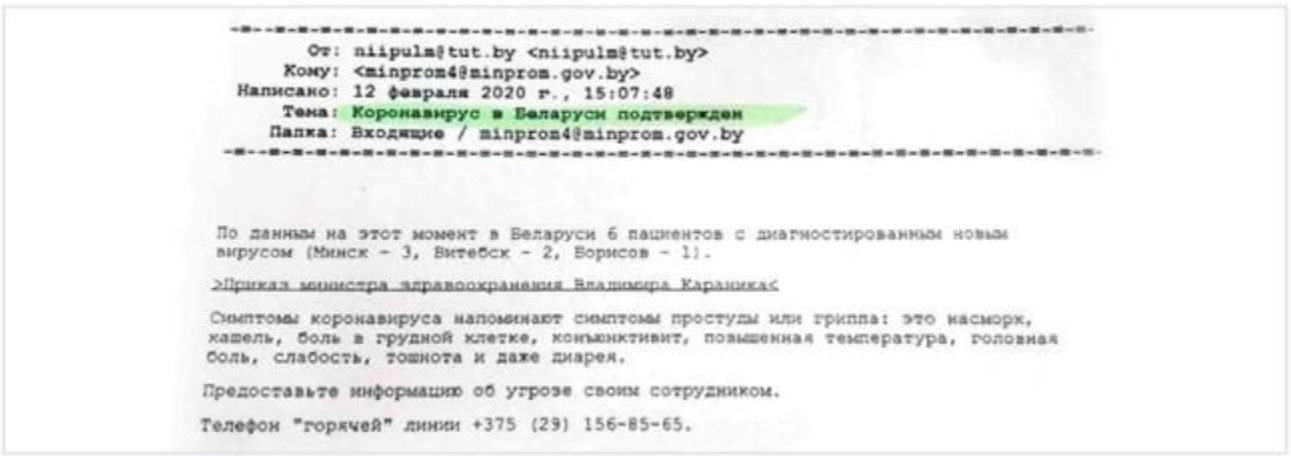
XDSpy - 2011 yılından bu yana hükümet sırlarını çalmaya çalışıyor

XDSpy APT grubunun büyük ihtimalle en karakteristik özelliği, dokuz yıl boyunca neredeyse hiç fark edilmemesidir. Bu casusluk grubu, 2011 yılından beri aktiftir ve etkinlikleri 2020 Şubat ayında Belarus Bilgisayar Acil Durum Müdahale Ekipleri (CERT) tarafından bir *raporda* belirtilene kadar belgelenmemiştir.

Grup, yıllar içinde Doğu Avrupa'daki ve Balkanlardaki askeri kurumlar, Dış İşleri Bakanlıkları gibi birçok hükümet kurumuna ve özel şirketlere sızmıştır. ESET telemetrisine göre XDSpy'ın hedefleri Belarus'ta, Moldova'da, Rusya'da, Sırbistan'da ve Ukrayna'da yer alır.

Özelikle iki olayda, XDSpy operatörleri, kimlik avı dolandırıcılığı kampanyalarında COVID-19 temasını kullanmıştır. 2020 Şubat ayında, ilk COVID-19 vakalarının Belarus'ta görüldüğünü belirten bir e-posta yoluyla kötü amaçlı yazılım yaydılar. Hatta ülkede resmi olarak bildirilen vakalar bu tarihten birkaç hafta sonraydı. Beklenmeyen bir yanlış bilgi kampanyasının parçası olarak sosyal ağlarda dolaşan kötü amaçlı bu e-postanın fotoğrafı aşağıda yer alıyor.

Daha sonra 2020 Eylül ayında operatörleri, COVID-19 ile ilgili resmi bir Rusya hükümet internet sitesi olan rospotrebnadzor.ru sitesini, XDDown indirmek için bir tuzak olarak kullandı. Bu ana kötü amaçlı yazılım bileşeni, diğer eklentileri indirmek üzere kullanılır.



От: niipulm@tut.by <niipulm@tut.by>
Кому: <minprom4@minprom.gov.by>
Написано: 12 февраля 2020 г., 15:07:48
Тема: Коронавирус в Беларуси подтвержден
Папка: Входящие / minprom4@minprom.gov.by

По данным на этот момент в Беларуси 6 пациентов с диагностированным новым вирусом (Минск - 3, Витебск - 2, Борисов - 1).

>Приказ министра здравоохранения Владимира Караника<

Симптомы коронавируса напоминают симптомы простуды или гриппа: это насморк, кашель, боль в грудной клетке, конъюнктивит, повышенная температура, головная боль, слабость, тошнота и даже диарея.

Предоставьте информацию об угрозе своим сотрудникам.

Телефон "горячей" линии +375 (29) 156-85-65.

İşlevsellik ve mimari açıdan XDSpy, istenen eylemleri gerçekleştirmek üzere diğer eklentileri indiren bir ana indirme modülü içeren tipik bir siber casusluk araç seti kullanır. Araştırmamız esnasında ana C: sürücüsünden veya harici sürücülerden dosyaları çalmak, ekran görüntüsü almak ve internet tarayıcıları ile e-posta programları gibi çeşitli uygulamalarda kayıtlı parolalara ulaşmak için kullanılan eklentiler ortaya çıkardık. XDLoc adlı bir eklenti, yakındaki SSID'leri (Wi-Fi erişim noktası adları) toplamak üzere kullanılıyor. Bunun amacı büyük ihtimalle kurban olarak seçilen makinelerin coğrafi konumunu belirlemektir.

XDSpy operatörleri, hedeflerini suistimal edebilmek amacıyla kimlik avı dolandırıcılığı e-postaları kullanıyor. Bu e-postalar küçük farklılıklar gösteriyor. Bazıları zararlı bir dosyaya bağlantı içerirken, diğerleri ise ek içeriyor. Zararlı dosya veya ekin ilk katmanı genellikle bir ZIP veya RAR dosyasıdır. 2020 Haziran ayının sonunda operatörler, Internet Explorer'ın bir açığı olan CVE-2020-0968'i kullanarak saldırılarını bir üst noktaya taşıdı.

Fransa'daki Exaramel arka kapısı: Başka bir Sandworm tedarik zinciri saldırısı mı?

Kötü bir şöhrete sahip Sandworm APT grubu söz konusu olduğunda, geçtiğimiz son altı aydaki en önemli haber, kuşkusuz ABD Adalet Bakanlığı tarafından, altı Rus Dış İstihbarat Servisi görevlisinin grubun birçok saldırısında yer aldığının ileri sürüldüğü *iddianamedir*.

Jeopolitik tarafını bir yana bırakırsak, Sandworm'un en ünlü saldırıları 2015 (*ilk Ukrayna enerji şebekesi saldırıları*) ve 2018 (*Olimpik Yok Edici*) yılları arasında olsa bile savunmacılar, bu tehlikeli grubun 2021'de halen oldukça aktif olduğunu unutmamalıdır.

2021 Şubat ayında Fransa'nın ulusal bilgi güvenliği ajansı ANSSI bir *rapor* yayınladı. Bu rapora göre Centreon BT izleme yazılımını hedef alan bir güvenlik ihlali söz konusuydu ve bunun sonucunda birçok Fransız kuruluşuna sızıldı.

Kampanya 2017'den 2020'ye kadar sürdü ve web barındırma sağlayıcıları başta olmak üzere birçok BT sağlayıcı etkilendi. İhlale uğrayan sistemlerde iki arka kapı keşfedildi: P.A.S. web kabuğu ve (daha da ilginci) *Exaramel* arka kapısı.

Exaramel, Sandworm grubunun (özellikle ESET'in TeleBots olarak izlediği bir alt grubun) çalışmasıdır ve kod benzerliklerine dayanarak kötü bir üne sahip olan *Industroyer*'ın da aynı APT grubuna ait olduğuna dair kanıt sunar.

Geçtiğimiz aylardaki SolarWinds saldırısı göz önünde bulundurulduğunda, Sandworm'un geçmişte tedarik zinciri saldırıları (NotPetya salgınına neden olan *M.E.Doc ihlalini* hatırlıyor musunuz?) düzenlediği gerçeği yüzünden siber güvenlik sektörü, Centreon ihlalinin ayrıntılarını derhal öğrenmek istedi.

Centreon'a göre ihlal, bir tedarik zinciri saldırısının sonucu değildi. Kampanya, şirketin kendisine değil de BT izleme yazılımının güncel olmayan sürümlerine sızıyordu.

Bunun bir tedarik zinciri saldırısı olmaması olumlu bir durumdur, çünkü böyle bir saldırı potansiyel olarak oldukça geniş çaplı sonuçlara sahip, ciddi bir ihlale işaret eder. Ancak başka bir gerçek de söz konusudur: Centreon BT izleme yazılımının güvenlik açığına sahip sürümünü kullanan kuruluşlar var ve saldırganlar bu kuruluşlara sızmak amacıyla bu durumdan yararlanıyor.

Geleceğe bakış

Geçtiğimiz altı ay içinde Sandworm gibi oldukça karmaşık olanlardan XDSpy gibi daha az yetkin (yine de radarlara yakalanmayıp hedeflerine ulaşabilecek durumda) olanlara kadar birçok APT grubu, her zamanki çalışmalarına devam etti.

SolarWinds saldırısı (veya geçtiğimiz günlerde gerçekleşen ve tedarik zinciri saldırısı olmasa da tedarik zinciri saldırısına benzeyen Centreon olayı gibi diğer olaylar) kadar zarar vermese de tedarik zinciri saldırıları yaygın bir akım olmaya başladı. ESET, sektörün tamamında birkaç yıl önce tüm yıl boyunca karşılaşılan tedarik zinciri saldırısı miktarının 2020'nin yalnızca son çeyreğinde gerçekleştiğini ortaya çıkardı. Güney Kore'de hükümet ve bankacılık internet siteleri tarafından kullanılan *WIZVERA VeraPort* yazılımını ihlal eden Lazarus vakası, Moğolistan'ın çeşitli hükümet ajansları tarafından kullanılan Able Desktop sohbet yazılımını ihlal eden *StealthyTrident Operasyonu*, Vietnam hükümeti tarafından kullanılan sertifika dağıtma yazılımını ihlal eden *SignSight Operasyonu* bu saldırıların örneklerindendir. Ayrıca, daha bir kaç ay önce, 2021 yılının ilk çeyreğinde ESET, çevrimiçi oyun topluluklarını hedef alan bir tedarik zinciri saldırısı olan *NightScout Operasyonu*'nu da ortaya çıkardı.

Tedarik zinciri saldırılarını tespit edip önlemenin ne kadar zor olduğunu ve APT aktörleri ile siber suçluların bunlardan ne kadar büyük kazanç sağladığını göz önünde bulundurduğumuzda, bu gibi saldırıların yakın gelecekte Avrupa'da ve dünya genelinde artış göstereceğini tahmin etmek zor değildir.

Bu nedenle, güvenlik açığına sahip yazılım tedarik zincirlerinden kaynaklanan riskleri azaltmak üzere aşağıdakilere uymanızı tavsiye ediyoruz:

- Yazılımınız hakkında bilgi sahibi olun: Kuruluşunuzda kullanılan tüm açık kaynak ve özel mülk standart araçların envanterini tutun.
- Bilinen güvenlik açıklarına dikkat edin ve piyasaya sürülen tüm yamaları uygulayın; yazılımdan etkilenen güncellemeleri içeren saldırılar, hiç kimseyi yazılımını güncellemekten alıkoymamalıdır.
- Üçüncü taraf yazılım satıcılarını etkileyen güvenlik ihlallerine karşı dikkatli olun.
- Gereksiz veya eski sistemlerden, hizmetlerden ve protokollerden kurtulun.
- Güvenlik süreçlerini gözden geçirerek tedarikçilerinizin risklerini değerlendirin.
- Yazılım tedarikçileriniz için güvenlik gereksinimleri belirleyin.
- Düzenli kod denetimleri isteyin ve güvenlik kontrolleri hakkında bilgi edinin, ayrıca kod bileşenleri için kontrol prosedürlerini değiştirin.
- Potansiyel tehlikeleri belirlemek üzere sızma testleri hakkında bilgi edinin.
- Yazılım geliştirme süreçlerini korumak ve iletişim hattı oluşturmak üzere erişim kontrolleri ve iki faktörlü kimlik doğrulama (2FA) talep edin.
- Çok katmanlı korumaya sahip güvenlik yazılımı kullanın.

3

BT GÜVENLİĞİ VE HÜKÜMET: HEDEF ALINAN KURULUŞLAR ARASINDAKİ BENZERLİKLER

Bir siber güvenlik şirketinde bilgi güvenliği yöneticisi olmak eşsiz bir pozisyondur. Güvenlikle ilgili teknik alanlarda bilgiyle donatılmış bir yönetim ekibiyle çalışmak kuşkusuz çok faydalıdır. Ancak, siber güvenlik şirketleri de siber suçlular için bir hedef (hatta bir ödül) teşkil eder. Siber suçluların hedefinde olduğunun farkında olmamız, hükümet kuruluşlarıyla deneyimlerimizi paylaşabileceğimiz en önemli noktalardandır. Bu temel nokta ESET'te bilgi güvenliği yöneticisi olarak görev yaptığım 10 yıl boyunca hep geçerliydi ve çevrimiçi ortamın sürekli değişen talepleri karşılama konusunda güvenlikle ilgili tutumumuzu geliştirirken bu noktayı hep ön planda tuttuk.

Daniel Chromek
Bilgi Güvenliği Yöneticisi/Bölüm Sorumlusu

Ayrıca, hedef durumunda olmamızın, şirketimizin güvenlik kültürü, büyümesi ve iş modeliyle de güçlü bir bağlantısı vardır. Hükümetler de benzer bir zorlukla karşılaşır. Açık hedeftirler, her zaman düşmanları olacaktır ve tehdit dünyasındaki taktiklerin ve tekniklerin en kötü semptomlarının zararlarını hafifletmeye çalışmak, güvenlik politikasından kültüre ve stratejik büyümeye kaynak ayırmaya kadar her şeyi etkiler.

Gelişimin nasıl yapılacağına yönelik sorular, hem ESET'in bakış açısına göre hem de daha geniş bir bilgi güvenliği dünyasının bakış açısına göre cevaplanabilir. ESET ile ilgili daha fazla bilgi sahibi olduğumdan, "nasıl" sorusunu bu bakış açısıyla ele almam daha kolaydır. ESET, görev aldığım süre boyunca büyük bir büyüme gösterdi. Ayrıca şirket içi süreçleri, iletişimi ve bilgi alışverişini kolaylaştırmak amacıyla standardizasyon ve düzgün bir yönetim çerçevesine gereksinim duyan birçok etkinliğin olduğu, birbirine bağlı bir topluluktur.

Özellikle ESET'teki standardizasyon ve yönetim sayesinde, odak noktamızı öncelikle tüketici ve KOBİ müşterilerini korumaktan kurumsal segmentte önemli bir büyüme sağlamaya kaydırabildik. Bu destek, bilgi güvenliğini belgelendirmemizi, net direktiflere ve düzenlemelere uymamızı ve şirket ortamlarındaki güvenlik çözümlerini uygularken kurumsal müşterilerin sorularını ve tereddütlerini ele alma konusundaki becerilerimizi geliştirmemizi sağladı. Tüm hükümetlerin hizmetlerini dijitale dönüştürmek, iç süreçlerini iyileştirmek ve bunları daha iyi bir yönetimle resmileştirmek konusunda büyük bir taleple karşılaştığının farkındayız. ESET'in deneyimine benzer şekilde yönetim yoluyla süreçleri (ve kültürü) resmileştirme yolculuğu, yeni pazarlara ulaşma arzusunu ve hırsını içerir; hükümetler söz konusu olduğunda ise iyileştirilmiş büyüme, daha iyi hizmet tedariği, ulusal veya yerel tutarlılık bu yolculuğa dahildir.

Olgunlaşmanın etkileri

Şüphesiz, şu anki olgunluk seviyesine ulaşmadan önce de yönetimle ilgili zorluklar mevcuttu ve şirketin büyümesiyle bu zorluklar daha karmaşık hale geldi. Karmaşık bir BT ortamında güvenlik kontrollerini kullanıma almak, eskisine kıyasla çok daha fazla zaman ve kaynak gerektiriyor. Bu nedenle, iç güvenlik bölümümüz önemli ölçüde büyüdü ve şu anda çeşitli güvenlik alanlarına odaklanan farklı ekipler içeriyor.

Ayrıca yönetime yapılan sunumlar, rahatlıkla ayrıntılı teknik incelemelere dönüşebileceğinden iç güvenlik bölümü çok iyi hazırlanmış olmalıdır. Bu şekildeki en son ayrıntılı incelememiz, yönetimin bildirmeye uygun olup olmadığını anlaması amacıyla güvenlik açığı yönetim aracımızın risk skor parametresi ve bunun arkasındaki formülle ilgiliydi. Bu inceleme, kötü amaçlı yazılım kitlerinde bir sızıntı olmasının, risk skorunu geleneksel CVSS skorlarının üstüne nasıl çıkaracağıyla ilgili bir tartışmayı içeriyordu. Bundan 12 yıl önce, güvenlik politikalarımızla ilgili tartışmalara kurucu ortaklarla birlikte katıldığım zaman olduğu gibi bugün de ESET'te derinlemesine incelemeler yapmak kültürel bir değerdir.

Şüphesiz, bilgi güvenliği yöneticisi görevine gelmemden önce de oldukça becerikli çalışanlara sahiptik ve meslektaşlarımız arasında güvenliği ve "Büyük Biradere" karşı görünürlüğü dengede tutmayla ilgili endişeler vardı.

ESET'in sahipleri, gizliliğe önem veren kişilerdi ve halen önem vermeye devam ediyorlar. Ayrıca, personelin morali üzerinde olası etkisinin de ilk günlerden beri farkındayız. Bu nedenle, ESET kültürünü pozitif bir güvenlik şirketi temeli üzerine yapılandırmak amacıyla yola çıktık ve korku, belirsizlik ve şüphe taktiklerinin işe yaramayacağı ve bunların tüm kuruluştaki meslektaşların saygısını kaybetmeyle sonuçlanacağı konusunda yönetim dahil olmak üzere herkesi ikna ettik.

Buna tamamen katılıyorum, çünkü hepimiz benzer bir seçimle karşılaşıyoruz: Güvenliği ve görünürlüğü başka bir bileşen olan güven ile dengelememiz gerekiyor. Bu ihtiyaç *COVID-19 pandemisinin ortaya çıktığı* 2020 yılında net bir şekilde anlaşıldı ve ESET'i (ve muhtemelen hepimizi) çoğumuz için tamamen beklenmedik olan bir güvenlik geleceğine taşıdı. COVID'in hüküm sürdüğü günümüzde, güvenlik alanında başarılı olmak için bazı temel şeylerin doğru yapılması gerekiyor. Bu durum güvenin ötesine geçiyor ve 2021 yılında bilgi güvenliği yöneticileri olarak güvenlikle ilgili akılda tutmamız gereken pratik alanları içeriyor. Benim için bu alanlar şunlardır:

1. **Evden çalışma modunda temel ilkelere bağlı kalın**

Bilgi güvenliğinde "öze dönmek" her zaman iyi bir tavsiyedir. Bu durum, COVID'i geride bıraktığımız bir dünya olmasını umduğumuz 2021 yılı için de geçerlidir. Yamalar, yedeklemeler ve uç nokta koruması, çalışanlar nereden çalışırsa çalışsın önemli alanlardır. Birçok önlemin yanı sıra kuruluşun platformlarına daha güvenli bir şekilde erişim sağlamak üzere personel VPN hesaplarının genişletilmesi ve yönetimi önemlidir. Sıfır Güven güvenlik yaklaşımını veya "güven ama doğrula" sözünü akılda bulundurmak, uzaktan çalışma gereksinimlerini ele alırken yararlı olabilir. Bunları göz önünde bulundurun ve iyileştirmenin yollarını arayın.

2. **Kuruluşu yasal düzenleme kapsamındaki alanlarda genişletin**

Yalnızca ESET ile ilgili yorum yapabilecek durumda olsam da dünya genelinde güvenlikle ilgili düzenlemelerde hızlı bir artış olduğunu görüyoruz. Bu durum, COVID dolayısıyla hız kazanan dijitalleşmeyle birlikte giderek artacaktır. Örneğin, NIS Direktifi (ve *NIS2 Direktifi*) bir güvenlik sağlayıcı olarak ESET'i ve özellikle yasal düzenleme kapsamındaki sektörlerde faaliyet gösteren veya doğrudan hükümete hizmet sunan birçok ESET müşterisini etkiler. Bu nedenle, ortak yaklaşımlar oluşturmak üzere bir arada çalışmamız mantıklıdır.

Yalnızca geçen sene, COVID kısıtlamaları süresince ESET ve ESET ürünleri, ESET PROTECT Cloud gibi bulut hizmetlerimizin başlamasıyla birlikte yeni bir yasal düzenleme alanına girdi. Bu durum, ESET'in NIS Direktifi'ne uyum sağlaması ve ESET'in iş ortaklarının bulut tabanlı güvenlik yazılımı kullanımını düzenleyen yerel yasalara uygun bir şekilde hareket etmesi gibi çeşitli karmaşık durumları da beraberinde getirdi. Dolayısıyla NIS Direktifi gibi tek bir düzenlemeye uyum sağlamak çok hoş bir durum olmayabilir, ancak bu, hükümetin, sektörün ve kurumsal müşterilerin koyduğu birçok düzenlemeye ve standarda uymaktan çok daha kolay bir yoldur.

Bu zorlukların üstesinden gelmenin en iyi yolu ise temel bilgi güvenliği süreçlerinizi yönetmek üzere bir bilgi güvenliği yönetim sistemi (örneğin ISO 27001) kurmak ve daha sonra kuruluşunuzun uyum sağlaması gereken diğer güvenlik kontrollerini sistematik olarak eklemektir. Olgun Güvenlik Tesisi Modeli'nin (BSIMM) yanı sıra ISO 27001, kuruluşlara güvenlik yönetim sistemlerini ve iç kontrollerini geliştirmek ve bunların iyi bir şekilde dokümantasyonunu sağlamak konusunda yardımcı olabilir; bu durum uyumluluğu kanıtlamak için bir gerekliliktir.

3. Ekibin sağlıklı bir şekilde çalışmasını sağlarken çeşitli iş inisiyatiflerini desteklemek üzere kaynaklar arasında denge kurun

Sektör olarak bu noktada sıkıntı yaşadığımızı düşünüyorum. Herhangi bir olgun güvenlik programının karşılaştığı temel sorun, kuruluştaki birçok etkinlikle arasındaki ilişkidir; gerçekten önemli etkinliklere öncelik verme konusunda zorluklar yaşanır. Raporlama ve ölçme, bu durumu daha da karmaşık hale getirir. Riskler değerlendirilmeli, sonuçlar ve olaylar denetlenmelidir; geri bildirim alınmalı ve alınan dersler incelenmelidir; uyumlulukla ilgili sıkıntılar belirlenmelidir; buna benzer birçok durum söz konusudur. Hatta bazen karşılaştırılması mümkün olmayan şeyleri karşılaştırmamız isteniyor gibi düşünürüz. Aynı zorluk hükümet kuruluşları için de geçerlidir. Hükümet kuruluşları da iç mekanizmaların ve dış hizmetlerin güvenliği arasında raporlama ile denge kurmaya çalışır. Bütün bunlar hem uyumlu olmalı, hem de pratik bir şekilde işlevsel olmalıdır.

Ancak bu dengeyi sağlamanın en az iki yolu vardır. İlki, şirket önceliği yoludur. Şirketler önceliklerini belirlediği takdirde iç güvenlik kaynaklarını şirketlere kaydırmak kolaydır. Ancak şirket önceliklerini belirleyemezse (genel olarak veya diğer şirket birimlerinin önceliklerine kıyasla), bir çözüm bulmak üzere aşağıdaki soruları sormak gereklidir:

Risk nedir? Güvenlik ekibimiz şirketin iş inisiyatifini desteklemek üzere kaynak ayıramazsa risk nedir? Belli bir denetlemenin sonucunda elde edilenler kapatılamazsa risk nedir? …olmazsa risk nedir? Rekabet halindeki etkinliklerin önceliğini belirlerken risk, tek başına bir ölçme aracı olarak kullanılabilir.

4. Yazılım geliştirme yaşam döngünüzün olgunluğunu artırın

Kurumsal dünyada hayati öneme sahip sistemleri, ürünleri veya hizmetleri oluşturan, özelleştiren ve koruyan şirket içi ve dışı geliştirme ekiplerinin olması oldukça yaygın bir durumdur. Yazılım geliştirme yaşam döngüsünde kullanılan birden çok güvenlik standardı olması durumunda, bir şelale modelinin uygulanmasını beklemek karşılaşılan bir sorundur. Ancak, günümüz sektör koşullarında hızlı ve çevik bir şekilde geliştirme ve dağıtım baskısı varken DevOps etkinliklerinde bir şelale yaklaşımı uygulanabilir değildir.

ESET'in yaklaşımı, geliştirme ve operasyonlarla ilgili olan DevOps güvenlik etkinliklerini tanımlamak ve bu etkinlikleri metodolojilerine ve çalışma prosedürlerine nasıl dahil edeceklerini belirlemek üzere geliştirme ekipleriyle yakın bir ilişki kurmaktır. Buradaki amaç, şirket içindeki güvenlik uzmanlarının ve çeşitli geliştirme ekiplerindeki güvenlik uzmanlarının neler sunması gerektiğini belirlemek ve mümkün olduğunca otomasyon sağlamaktır.

5. Giderek daha karmaşık hale gelen saldırılara karşı hazırlıklı olun ve bu saldırılara tepki verin

Yıllar içinde *Verizon'un veri sızıntısı raporlarını* incelediğimizde, saldırıların gün geçtikçe daha kötü bir hale geldiğini görüyoruz. Bir sonraki seferde hangi güvenlik açıklarının ihlal edileceğini, saldırganların hangi araçları kullanacağını veya saldırganın amacının ne olacağını bilmiyoruz. Ancak, teknik açıdan katmanlı kontrollerle ve kurumsal açıdan olay tepki ekibinin sahip olduğu özelliklerle, becerilerle ve genel anlamda olgunlukla saldırılara karşı hazırlıklı olabiliriz.

COVID-19'un ortaya çıkardığı durum, her şeyin ne kadar hızlı değişebileceğini bizlere gösterdi. COVID'in ESET'te neden olduğu hızlı değişikliklere benzer değişiklikler, büyük olasılıkla diğer kuruluşlarda da yaşanıyor. Bu deneyimden benim çıkardığım başlıca dersler şunlardır:

- Çalışanlar, kuruluşun şirket içi ağının dışında, evden çalıştığından, varlık sınıflandırmasına ve uç nokta görünürlüğüne daha fazla odaklanmalıyız.
- Bulut tabanlı hizmetler kullanılıyorsa, diğer bulut güvenliği önlemlerinin yanı sıra doğru yapılandırmayı, erişim yönetimini ve kaynak ayırmayı önceliklendirmeliyiz.

Kendi deneyimlerimize göre saldırılarda açık bir şekilde artış vardır; özellikle Kurumsal E-posta Tehdidine (BEC) her zamankinden daha fazla rastlıyoruz. Neyse ki, uç nokta portföyümüzde, yeni ortaya çıkan tehditlere karşı sağlam bir kötü amaçlı yazılımdan koruma altyapısı ve bulutta yönetilen bir sandbox çözümü olan *ESET Dynamic Threat Defense* ile uç noktalara yönelik yoğun görünürlük sağlayan ve olaylara tepki verme becerilerimizi artıran bir uç nokta algılama ve tepki çözümü olan *ESET Enterprise Inspector* yer alır. Ayrıca Safetica ile teknoloji ortaklığımız sayesinde kullanımı kolay bir Veri Kaybı Önleme çözümüne de sahibiz.

Hedef alınsa da özenli

Saldırganların hedefinde olmaya devam ediyoruz, ancak yukarıda bahsettiğimiz bileşenler ve yönetime yoğun bir şekilde odaklanmamız sayesinde sağlam bir temele sahibiz. Bu temel, adli kanıtlar gibi belirli sorunlara odaklanmamıza ve elde ettiğimiz sonuçlarla kendi ürünlerimizde çalışmamıza olanak tanıyor. Bu noktada kötü amaçlı yazılım araştırması konusundaki deneyimimizle, ürün geliştirme becerilerimiz net bir şekilde örtüşüyor. Temel tespit teknolojilerimizle birlikte ESET Enterprise Inspector çözümümüzü kullanarak, aynı anda şirketi koruyabiliyor ve günün zorluklarını aşmak üzere sistemlerimizi, kültürümüzü ve süreçlerimizi sürekli olarak geliştirebiliyoruz.

4

EMISSARYSOLDIER: APT GRUBU LUCKYMOUSE'UN 2020 YILINDAKİ KÖTÜ AMAÇLI ETKİNLİKLERİ

LuckyMouse, Orta Asya'daki ve Orta Doğu'daki hükümet ağlarına ve özel şirketlere (telekomünikasyon, medya ve bankalar) sızıyor.

Matthieu Faou
Kötü Amaçlı Yazılım Araştırmacısı

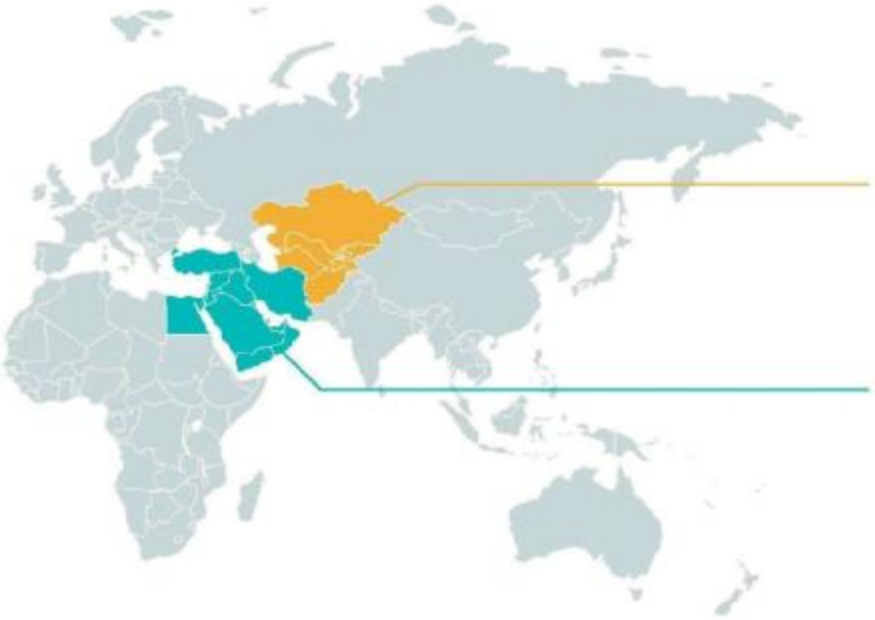
APT27 ve Emissary Panda olarak da bilinen LuckyMouse bir siber casusluk grubudur. Su kaynağı saldırılarını veya stratejik internet güvenlik açıklarını düzenli olarak kullanmasıyla tanınır. Grup, Orta Asya'daki ve Orta Doğu'daki birçok hükümet ağına sızmanın yanı sıra Uluslararası Sivil Havacılık Örgütü (ICAO) gibi uluslararası kuruluşlara da sızar.

ESET Research, LuckyMouse ile ilgili yaptığı son analizde 2020 yılında gerçekleşen birçok kötü amaçlı etkinlik ortaya çıkardı ve bu etkinliklerde operatörlerin temel olarak SysUpdate (Soldier olarak da bilinir) araç kitini kullandığını fark etti. ESET, bu etkinliklere EmissarySoldier adını verdi.

LuckyMouse, kurbanlarını suistimal etmek üzere genel olarak su kaynağı saldırılarını kullanır ve bu sayede hedeflediği kurbanların ziyaret edebileceği internet sitelerine sızar. Ayrıca, LuckyMouse operatörleri hedefteki kurbanları tarafından yürütülen internete açık ve güvenlik açığı bulunan sunucuları bulmak üzere ağ taramaları da gerçekleştirir. Grup, yama uygulanmamış sunuculara sızmak için genellikle bilinen güvenlik açıklarını kullansa da ESET, diğer tehdit gruplarıyla birlikte LuckyMouse'un da e-posta sunucularına saldırı düzenlemek için halen sıfır gün saldırısıyken Microsoft Exchange güvenlik açıklarını suistimal ettiğini fark etti.

LuckyMouse operatörleri makineye giriş sağladıktan sonra, özel sızıntı sonrası implantları olan SysUpdate veya HyperBro'dan birini yerleştirir. Araç kitleri arasındaki ilginç bir benzerlik ise tümünde tespit edilmemek üzere DLL arama sırası saldırısı bulunmasıdır.

2019 ve 2020 yıllarında bu uygulamada çeşitli uzaktan kod yürütme güvenlik açıkları bulundu. ESET'in elinde bu sızıntıların kullanıldığına dair kanıt olmasa da LuckyMouse bileşenlerinin Microsoft SharePoint'e de hizmet eden internet bilgi servisleri (ISS) yoluyla yerleştirildiğini gözlemledik.



görüntü: ESET telemetrisine göre, LuckyMouse 2020 yılında bu kurumları hedef aldı

Günümüzde Orta Doğu'da birçok casusluk grubu görülüyor ve LuckyMouse da bu bölgede oldukça aktiftir. Aynı makinede veya en azından aynı ağda birden çok tehdit aktörüyle karşılaşmak oldukça yaygındır. Bu bölgede LuckyMouse, genel olarak hükümet kurumlarına odaklanır. Operatörler, mevcut jeopolitik durumla ilgili analizler elde etmeye çalışır. Ancak Orta Asya'daki hedeflerinin çoğu özel şirketlerdir (telekomünikasyon, medya ve bankalar). Bu durum bölgedeki ekonomik durumun stratejik önemini gösterir.

LuckyMouse VPN düğümleri, kademelendirme düğümleri, komuta ve kontrol (C&C) düğümleri ile oldukça büyük bir ağ altyapısına sahiptir. EmissarySoldier kampanyası esnasında ESET, 16 farklı kademelendirme ve C&C düğümü gözlemledi.

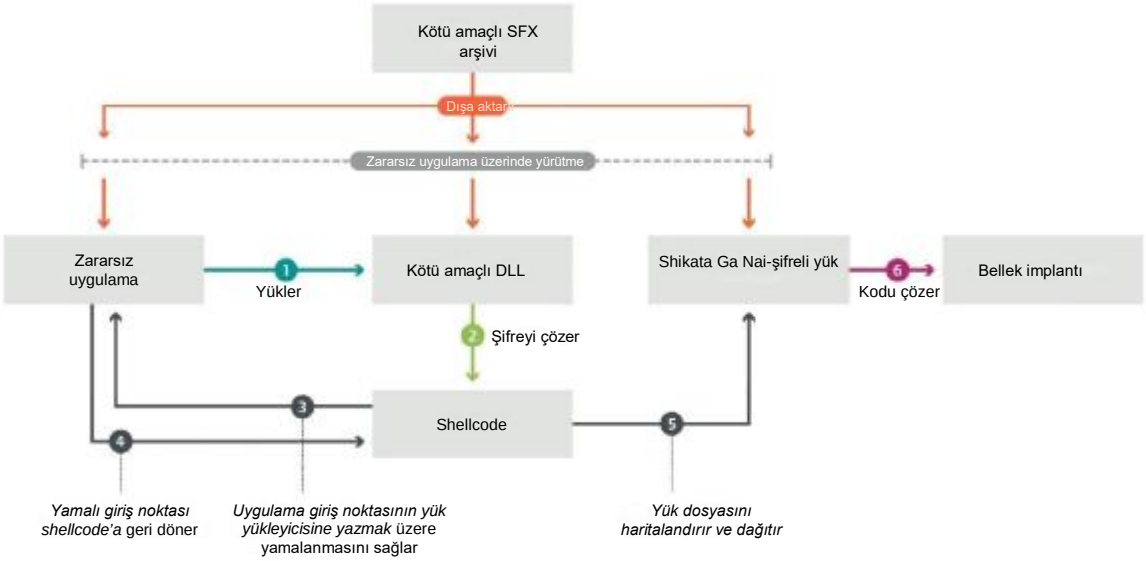
Ayrıca ESET araştırmacıları, ihlale uğrayan bazı makinelerde, internetten ulaşılabilen Microsoft SharePoint kullanıldığını fark etti.

LuckyMouse, implantlarını kurmak üzere SysUpdate araç kitinde üç çatallı model denilen özel bir yöntem kullanır. Üç çatallı modelde, DLL korsanlığına açık yasal bir uygulama, yükü yükleyen özel bir DLL ve işlenmemiş bir Shikata Ga Nai-şifreli ikili yük bulunur.

Üç çatallı modele genel bakış

Maddi kazanç elde etmenin yanı sıra casusluk amacı taşıyan tehdit aktörlerinde genelde görüldüğü üzere LuckyMouse, saldırgan güvenlik araçları kullanır. Bu nedenle, grup genellikle özel arka kapılar kullanırken ESET araştırmacıları bazı sızıntılarda grubun başka araçlar da kullandığını fark etti. Bu araçlar arasında şunlar bulunur:

- Yetki yükseltme aracı, JuicyPotato;
- Şifreler dahil olmak üzere çeşitli Windows sırlarını dışa aktaran, Mimikatz;
- NetBIOS tarayıcı, nbtscan.



LuckyMouse etkinliğiyle ilgili bu en son incelemede ele alınan SysUpdate araç kitinin kendisi nispeten yenidir; ilk örnekleri 2018 yılında görüldü. O zamandan bu yana araç kiti çeşitli gelişim aşamalarından geçti. Önceki örneklerden farklı olarak 2020 yılında kullanılan örneklerde büyük gelişmeler ve ek işlevler mevcuttur. Bu gelişmeler ve işlevler dahilinde birden çok C&C iletişim protokolü uygulanmıştır ve mevcut özelliklerde küçük iyileştirmeler bulunur.

SysUpdate bileşenleri, her biri operasyonel amaca sahip bir dizi ikili dosyaya bölünmüştür. SysUpdate'in üç çatallı modelinde, GUP.exe gibi zararsız bir uygulama bulunur. Bu uygulama bir sonraki bileşen olan DLL'nin ilk yükleyicisi olarak çalışır. Sonraki bileşen olan DLL ise bir sonraki bileşen olan Aşama 1 yükün yükleyicisi olarak çalışır. Bu üç bileşen, ihlal edilen sisteme ilk erişim sağlanırken herhangi bir konuma yerleştirilir. Bu yöntemin farklı bölgelerdeki farklı kurbanlarda yinelenen bir etkinlik olduğu gözlenmiştir.

SysUpdate oldukça modüler olduğundan, operatörleri isteğe bağlı olarak çeşitli kötü amaçlı özellikleri kullanabilir. Ayrıca isteğe bağlı olarak kötü amaçlı yazılımın görünürlüğünü azaltabilir veya sınırlandırabilirler. Bu nedenden ötürü ESET araştırmacıları, kötü amaçlı modülü ele geçiremedi ve bu durumun SysUpdate'in kullanıldığı gelecek operasyonları analiz ederken de karşılaşacakları bir zorluk olduğunu düşünüyor.

Böylesine güvenilmez bir tehdit aktöründen uzak durmanın en iyi yolu, ağdaki şüpheli olayları belirlemek üzere bir uç nokta algılama ve tepki (EDR) çözümü kullanmaktır. Çeşitli özelliklerin giderek artan bir şekilde SysUpdate araç kitine eklenmesiyle bir araç yenileme sürecinden geçen LuckyMouse, 2020 yılında etkinliğini artırdı. Bu durum, LuckyMouse etkinliklerinin arkasındaki tehdit aktörlerinin, HyperBro kullanımından SysUpdate kullanımına kademeli olarak geçtiğinin bir göstergesi olabilir.

HyperBro, geçtiğimiz yıllarda tehdit istihbarat topluluğunun dikkatini çeken daha eski bir araç kitidir. Çeşitli APT grupları tarafından kullanıldığına dair birçok kanıt bulunur. Ancak SysUpdate, HyberBro kadar tanınmıyor; SysUpdate'in adının geçtiği yalnızca birkaç kamuya açık rapor bulunuyor. Büyük ihtimalle çok az sayıda operasyonda kullanıldı.

Son zamanlardaki kampanyalarda LuckyMouse'u ve araçlarını izlemek önceliklerimizdendir. ESET bu araştırmasına devam ettiği sırada e-posta sunucularına saldırmak ve SysUpdate araç kitini kurmak üzere tehdit grubunun *Microsoft Exchange sunucularındaki güvenlik açıklarını* ihlal etmesi bu önceliğin önemini vurguluyor. Bu durum, hükümetlere ve şirketlere internete açık sunucularındaki güvenliği sıkılaştırmalarını, güvenlik stratejileri konusunda daha fazla işbirliği halinde olmalarını ve EDR araçlarının kullanımında kapasitelerini ve olgunluklarını artırmalarını net bir şekilde gösterir.

5

DÜZENLEYİCİ RADAR: AB'DEKİ VE ABD'DEKİ SİBER GÜVENLİK TUTUMU İÇİN KRİTİK İPUÇLARI

Toplumun teknolojiyle olan ilişkisinin artmasıyla ve teknolojiyi art niyetli kullanmak isteyenlerin ortaya çıkmasıyla dünya genelinde hükümetler siber alanı düzenleme gayreti içerisine girdi. Hayati öneme sahip ulusal altyapıyı, kişisel bilgileri, güvenlik ve savunma varlıklarını korumak, hükümet kurumlarının sürekliliği sağlayarak sosyal istikrarın devamını sağlamak, şirketlerin ve diğer kuruluşların sorumluluklarını yerine getirmesini ve yaptıklarının sorumluluğunu üstlenmesini sağlamak amacıyla hükümetler, devlet tarafından desteklenen veya suç örgütlerine bağlı kötü aktörleri caydırmak üzere cezai yaptırımlar yoluna yöneliyor. Ayrıca hükümetler, siber güvenlik riskleri konusunda vatandaşları eğitmeyi ve zararı en aza indirmeyi de hedefliyor.

Andy Garth
Hükümetle İlişkiler Sorumlusu

Ülkelerüstü düzeyde ise Birleşmiş Milletler devlet etkinliğiyle ilgili uluslararası yasanın uygulanması konusunda sözleşmeyi sağlamaya ve 2015'te kabul edilen siber alanda sorumlu davranış olarak kabul edilen 11 normun oluşturulması konusunda çalışmalarına devam ediyor. Avrupa Birliği'nin 2018 yılındaki GDPR yönetmeliği, gizlilik ve güvenlik düzenlemelerini güçlendirmek isteyen ülkeler tarafından referans noktası olarak hızla benimsendi. AB'nin ve ABD'nin (yeni Biden yönetimi altında) önümüzdeki yıllarda siber alanda artan düzenlemeler konusunda söz sahibi olması bekleniyor.

Bu alanda küresel olarak kabul edilen standartların olmaması, düzenlemelerin bütünlüğüne zarar veriyor. Şu anda düzenlemeler, ulusal seviyede kamu ve endüstri sektörleri tarafından temel olarak sağlanıyor. İnovasyonun ve yasal karmaşıklıkların artmasıyla bu durum birçok hükümeti güvenlik zorlukları karşısında çaresiz bırakıyor ve birçok hükümet bunlara ayak uydurma konusunda zorlanıyor.

Siber alanın geniş kapsamını ve devletlerin farklı yaklaşımlarını göz önünde bulundurduğumuzda bilgi güvenliği yöneticileri ve politika yapıcılar, gelecekteki yasalara uygunluk ve güvenlik tutumları için kritik ipuçlarını takip etmek adına aşağıdaki alanları akılda bulundurmalıdır:

Avrupa Birliği: NIS2 Direktifi

AB, 2020 yılı Aralık ayında NIS2 Direktifi'nin taslak metnini yayımladı. Bu taslak uyarınca, siber güvenliği iyileştirmek üzere önlemlerini güçlendirmesi gereken kurumların ve sektörlerin sayısı önemli ölçüde artıyor. Şu anda bu metin, yasal inceleme sürecindedir.

Metnin son hali onaylandığında, direktifi uygulamak üzere üye devletlerin 18 ayı olacaktır. Bu durumun etkileri AB'de ve diğer ülkelerde hissedilecektir. **Önerilen NIS2 Direktifi şunları içerecektir:**

- Daha sıkı denetleyici önlemlerin alınması;
- Üye devletler arasında uyumlu yaptırım uygulamaları dahil olmak üzere daha sıkı uygulama gerekliliklerinin uygulanması;
- Ulusal seviyede ve AB seviyesinde siber kriz yönetimi konusunda bilgi paylaşımının ve işbirliğinin sağlanması;
- Kritik varlıkların dayanıklılığını sağlamak üzere ulusal stratejilerin oluşturulmasının zorunlu kılınması;
- Ulusal risk değerlendirmeleri düzenlenmesinin zorunlu kılınması;
- Tedarik zincirlerinin güvenliğinin güçlendirilmesinin hedeflenmesi.

NIS2 Direktifi benimsendiğinde, önerilen "Kritik Varlıkların Dayanıklılığı Direktifi" gibi sektöre özgü düzenlemeler de uygulanacaktır. Sektöre özgü bu düzenlemenin amacı, kritik altyapıyı korumak ve NIS2 Direktifi'nde belirtilen zorunluluklara denk bir etkiyle siber güvenlik risk yönetimi ve bildirim zorunluluklarını uygulama konusunda NIS2 Direktifi'nin tamamlayıcısı olmasıdır.

Avrupa Birliği: Siber Güvenlik Sertifikası

Şu anda yürürlükte olan 2019 AB Siber Güvenlik Yasası ile AB Siber Güvenlik Ajansı'na (ENISA) kalıcı olarak yetki verilmiş oldu. Bu yasa siber güvenlik sertifika çerçevesini belirlemede ve korumada ana rol oynar. Belirlenen gerekliliklere uygunluk seviyelerine dayalı olarak kullanıcılara güvence seviyeleri sunan bu çerçeve sayesinde kapsamlı kurallar, teknik gereklilikler ve prosedürler bakımından AB çapında sertifika şeması sağlar.

Ayrıca bu sertifika şemaları sayesinde bilgi ve iletişim teknolojisi (ICT) ürünlerinin ve hizmetlerinin güvenlik özelliklerinin değerlendirmesi, AB tarafından belirlenen düzenlemelere göre yapılır. Kısaca, bu yasa şu açılardan ICT ürünlerinin ve hizmetlerinin onay almalarını sağlar:

- Kapsamdaki ürün ve hizmet kategorileri;
- Siber güvenlik gereklilikleri;
- Değerlendirme türü;
- Beyan edilen güvence seviyesi.

ENISA ve Avrupa Komisyonu'na destek ve danışmanlık veren kuruluşlar şunlardır:

- Avrupa Siber Güvenlik Sertifika Grubu (ECCG);
- Paydaş Siber Güvenlik Sertifika Grubu (SCCG)
- Avrupa Siber Güvenlik Endüstri, Teknoloji ve Araştırma Yetkinlik Merkezi (ECCC).

Özellikle ECCC'nin siber güvenlik araştırma, yüksek teknoloji ve inovasyon alanında temel araç olması bekleniyor. Genel olarak bu misyon aşağıdaki hedeflere hizmet edecektir:

1. Ürünlerin ve çözümlerin tedariğini sağlamak.
2. Yeni kurulan şirketlere ve KOBİ'lere finansal destek ve teknik yardım sunmak.
3. Kapsamlı bir araştırma gündemine bağlı kalarak araştırma ve inovasyonu desteklemek.
4. Özellikle beceri geliştirme alanı başta olmak üzere yüksek siber güvenlik standartları koymak.
5. İkili teknolojiler (Avrupa Savunma Fonu ile ilişkili olarak) bakımından sivil ve savunma alanları arasında işbirliğini sağlamak.

Tony Anscombe
Kıdemli Güvenlik Misyoneri

ABD gizlilik düzenlemeleri ve değişen siber güvenlik yasaları

2018 yılında AB'nin GDPR yönetmeliğini yürürlüğe koymasının ardından, Amerika Birleşik Devletleri'nde de veri gizliliği düzenlemelerinin uygulanması devlet seviyesinde hız kazandı. Kaliforniya'daki yasa düzenleyiciler, 2018 yılında Kaliforniya Tüketici Gizliliği Yasası'nı çıkardı ve 2020 yılında bu yasa uygulanmaya başlandı. 2020 yılının sonlarında Kaliforniya'da Proposition 24 yürürlüğe girdi; Kaliforniya Gizlilik Hakları Yasası (CPRA) anlamına gelen bu yasa 2023 yılında uygulanmaya başlayacaktır. CPRA, bazı açılardan GDPR'ye göre eksik yönlere sahip olsa da birçok açıdan GDPR'den daha iyi olan CCPA'ya önemli eklemeler yapar. Bu eklemeler şunlardır:

- GDPR'de vurgulanan yalnızca bireysel verilere ek olarak hane halkı verileri kavramı;
- Kaliforniya'da ikamet edenlere, geçici nedenlerden ötürü eyalet dışındayken bile koruma sağlama;
- Kişisel verilerin üçüncü taraflara satılmasından cayma hakkı. Şirketler, web sitelerinin ana sayfalarında "Kişisel Bilgilerimi Satma" bağlantısı içermelidir. Veri sahibinin pazarlama amaçları doğrultusunda kullanıma izin vermeme ve ek olarak verinin işlenmesiyle ilgili etkinliklere rıza vermeme hakkı gibi konularla ilgili benzer korumalar GDPR'de yer alır ancak bu kadar net değildir.

2020 Nisan ayındaki Tüketici Çevrimiçi Gizlilik Hakları Yasası'nda (COPRA) yer alan federal tüketici gizlilik düzenlemesine ihtiyaç olduğuyla ilgili yaygın görüş ve Biden yönetiminin federal gizlilik düzenlemesine ihtiyaç olduğuyla ilgili beyanlarından yola çıkarak bu konuda girişimlerin olacağına inanıyoruz.

Ayrıca Başkan Yardımcısı Kamala Harris, gizlilik uygulamalarıyla ilgili sağlam bir geçmişe sahiptir. Harris'in Kaliforniya eyaleti Adalet Bakanlığı'nı yürüttüğü sırada Kaliforniya Çevrimiçi Gizlilik Koruma Yasası (CalOPPA) değiştirildi ve güçlendirildi. Ayrıca, Obama döneminde kanun tasarısına katkıda bulunan bazı çalışanlar da halen görevdedir.

Pandeminin devam ettiği günümüzde gözler sağlık hizmetleri sağlayıcıların ve temaslı izleme, test ve aşılama sağlayan ajansların üzerindedir. Şu anda durumun aciliyeti ve tıbbi gereklilikleri dolayısıyla kişisel verilerin toplanmasıyla ilgili bazı süreçler ayrıntılı bir şekilde ele alınamıyor olabilir. Ancak bu durum geçici olacağı ve bu gibi veriler için siber güvenliğin güçlendirilmesinin gerekliliği unutulmamalıdır.

Ayrıca internetin dünya genelinde sınırları ortadan kaldıran bir ortam oluşturduğu ve her şeyin aynı bulutta erişilebilir olduğu aşikardır. Gizlilik düzenlemeleri, sürekli olarak geliştirilmesi gereken bir süreçtir. Bu süreçte yapay zeka, Nesnelerin İnterneti ve teknolojideki diğer gelişmeler gibi yeni teknolojileri de göz önünde bulundurursak düzenlemelerin sürekli olarak gelişen koşullara göre uyarlanması gerekir. Dünya çapında eyaletler, ülkeler ve kıtalar arasında standardizasyona ve uyuma ihtiyaç vardır. Nerede olursa olsun şirketler ve kuruluşlar tüm tüketicilere aynı gizlilik politikası haklarını sunmalıdır. Gizlilik düzenlemeleri, tüm yasa düzenleyiciler için bir öncelik teşkil etmeye devam edecektir.

ABD'deki siber güvenlik yasaları

ABD'de toplumun genelini kapsayan siber güvenlik yasaları yürürlükte olmasına rağmen, genel olarak düzenlemeler şirketin veya kuruluşun sektörüne göre değişiklik gösterir. Ayrıca, bazı düzenlemeler, birden çok endüstri sektörünü içeren belirli teknolojilere yöneliktir.

Siber güvenlikle ilgili önde gelen sektöre özgü ABD düzenlemelerinden bazıları şunlardır:

- Sağlık Sigortası Taşınabilirlik ve Sigorta Yasası (HIPPA);
- Gramm-Leach-Bliley Yasası;
- Dodd-Frank Yasası;
- Nesnelerin İnterneti Siber Güvenlik İyileştirme Yasası.

- Tüketici Gizliliğini Koruma Yasası 2017: Şirketlerin kişisel bilgileri korumasını ve veri ihlali durumunda bildirimde bulunmasını gerektirir.
- Siber Güvenlik Bilgi Paylaşımı Yasası (CISA): Siber güvenlik tehditleri nedeniyle hükümet ve teknoloji şirketleri arasında internet trafiğinin paylaşılmasına olanak sağlar.
- Federal Bilgi Güvenliği Yönetimi Yasası (FISMA): Hükümet kurumlarının bilgi güvenliğiyle ilgili olarak politikalara, standartlara ve kılavuzlara sahip olmasını gerektirir.

Sektöre özgü düzenlemelerden biri HIPPA'dır. Bu düzenleme, sağlık hizmeti veren kuruluşların kişiyi tanımlamak için kullanılabilecek bilgileri dolandırıcılığa ve hırsızlığa karşı korumasını ve sağlık hizmeti sigorta kapsamındaki sınırlandırmaları ele almasını gerektirir. Finans sektöründe ise kuruluşların Gramm-Leach-Bliley Yasası'na ve Dodd-Frank Yasası'na uygun hareket etmeleri gereklidir. Bu yasalar, güvenlik tehditlerine ve veri bütünlüğü sorunlarına karşı bilgileri korumak üzere politikalar olmasını şart koşar.

Tüketici Finansını Koruma Bürosu, Dodd-Frank Yasası dahilinde olası yeni kurallar koyma yetkisine sahiptir. Bu doğrultuda 2020 yılı sonbaharında büro, Önerilen Düzenlemeyle ilgili bir Ön Bildirim yayınladı. Bu durum yakın gelecekte veriye tüketici onaylı erişim yöntemlerinde ve yasa uyarınca gerekli veri güvenliği seviyesinde değişikliklere neden olacaktır.

Nesnelerin İnterneti

Son olarak, 2020 yılında Nesnelerin İnterneti Siber Güvenlik İyileştirme Yasası çıktı. Bu yasa tüm sektörler için geçerlidir. Bu yasaya göre Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), hükümet sistemlerinde Nesnelerin İnterneti cihazlarının uygun şekilde kullanımında federal ajanslar için standartlar ve kılavuzlar yayımlamalıdır.

Bu şekilde bir Nesnelerin İnterneti düzenlemesi, ajansların aşağıdakilere uyması için aşamalı bir zaman çizelgesi içerir:

- Kullanımdaki cihazların güvenlik açıklarının nasıl ele alınacağı ve ortadan kaldırılacağıyla ilgili mutabakat sağlamak;
- Siber güvenlik risklerini yönetmek üzere minimum bilgi güvenliği gereksinimlerini belirlemek;
- Her beş yılda bir kılavuzları ve standartları gözden geçirmek ve düzeltmek.

Son madde 2022 Aralık ayında yürürlükte olacaktır ve NIST standartlarına ve kılavuzlarına uygun olmayan Nesnelerin İnterneti cihazlarının kullanımını bu tarihten sonra yasaklamaktadır.

6

UÇ NOKTA ALGILAMA VE TEPKİ: SÜREKLİ TEHDİTLERE KARŞI KOYMAK

Büyük kuruluşlar ve dış işleri bakanlıkları, elçilikler ve diğer diplomatik temsilcilikler gibi hükümet kuruluşları casusluk operasyonlarının ana hedefidir. Tehdit aktörleri, hassas bilgileri çalmak üzere çeşitli yollarla bu kuruluşları hedef alır. Başarılı olabilmeleri için hedef ağda mümkün olduğunca uzun bir süre görülmeden ve tespit edilmeden kalmak önemli olduğundan bu kötü amaçlı kampanyaların önemli bir parçası gizliliktir.

Uç nokta algılama ve tepki (EDR) teknolojisi, özellikle tamamen tespit edilemez kötü amaçlı yazılım veya yasal araçları kullanan gizli tehdit aktörlerinin şüpheli davranışları sürekli izleyerek bu aktörleri tespit etmek üzere büyük kuruluşlara yardımcı olabilir. EDR'ler saldırganlar tarafından suistimal edildiği bilinen popüler olmayan uygulamaların veya yasal araçların (örneğin living-of-the-land ikilileri (LOLBins) gibi) yürütülmesi durumunda uyarı verir. Bu sayede ağlarını savunanlar, ağlarındaki şüpheli etkinlikleri görebilir ve araştırabilir.

ESET araştırmacılarının yıllardır takip ettiği bir tehdit aktörü olan *Invisimole*, isminden de anlaşılacağı üzere casusluk amacıyla yüksek profile sahip kuruluşları hedefler ve mümkün olduğunca zor tespit edilebilmek üzere çeşitli stratejiler kullanır. Invisimole operatörleri bir kuruluşa girdikten sonra, erişimin sürekliliğini sağlamak üzere farklı kalıcılık zincirleri kurar. Ancak her ne kadar farklı zincirler kullansalar da ortak olan tek bir şey vardır: Diskte kötü amaçlı kod bulunmaz.

Ayrıca, Invisimole operatörleri casusluk etkinliklerini yerine getirebilmek için belleğe kötü amaçlı araçları yüklemek ve kurmak üzere yasal araçları suistimal eder. Bu yasal araçların kullanımı, standart algılama teknolojilerinin anormallikleri algılamasını zorlaştırır. Bu durumlarda gizlilik nihai hedeftir ve ağını savunmak isteyenler, bu gibi kötü amaçlı etkinliklerin algılanması ve doğru bir şekilde zararlarının azaltılması için düzgün bir biçimde yapılandırılmış bir EDR çözümüne güvenir.

7

ESET'İN UÇ NOKTA ALGILAMASI VE TEPKİSİ:

UÇ NOKTA ALGILAMA VE TEPKİ NEDİR?

Uç nokta algılama ve tepki (EDR) çözümleri, uç noktalardaki etkinlikte oluşturulan büyük miktardaki veriyi toplar ve analiz eder. Şüpheli davranışlar, güvenlik profesyonellerini uyaran bir alarma neden olur; bu sayede güvenlik profesyonelleri bu davranışları araştırır ve aksi takdirde gözden kaçabilecek olası saldırıları ortaya çıkarır. ESET, Windows ve macOS uç noktalarını koruyabilecek bir EDR çözümü olan ESET Enterprise Inspector'ı (EEI) geliştirdi.

MITRE ATT&CK®

ESET Enterprise Inspector, kötü amaçlı taktikleri, teknikleri ve prosedürleri algılamak amacıyla MITRE ATT&CK bilgi tabanını referans alır. Bu bilgi tabanı siber alandaki en karmaşık tehditler ve kötü amaçlı gruplar hakkında kapsamlı bilgiler sunar. Bu bilgi tabanına sağladığı 20'den fazla katkıyla ve üçüncü *MITRE Engenuity ATT&CK Değerlendirmeleri*'ne sağladığı katılımla EDR çözümümüz, gerçek ortamlarda test edilmiştir ve olgunlaşmıştır.

Tehdit avlama

Şüpheli davranışları algılamak için zor koşullar altında test edilen bir dizi kurala ve dosyanın popülerliğine, geçmişine, imzasına, davranışına ve diğer bağlamsal bilgilerine dayalı olarak verileri sıralamak üzere gelişmiş filtreleme becerilerine sahip EEI, hedeflenen saldırıları ortaya çıkarmak için otomatik ve kolay tehdit avlama özelliği sunar.

EEI özel kuralların oluşturulmasına ve kural harici durumlara olanak tanıdığından, bir ortama en iyi şekilde uyum sağlamak veya tehdit avı için özel yapılandırmalarla olay veritabanını yeniden taramak üzere ayarlanabilir.

Halka açık API

ESET Enterprise Inspector, güvenlik mühendislerinin algıladıkları kötü amaçlı yazılımları dışa aktarmasına olanak tanıyan bir API özelliğine sahiptir. Bu sayede SIEM, SOAR, destek sistemi ve diğer araçlar ile etkili bir şekilde entegrasyon sunar.

ESET HAKKINDA

ESET® dünya çapında 30 yılı aşkın bir süredir şirketleri, önemli altyapıyı ve dünya genelindeki tüketicileri gittikçe artan karmaşık dijital tehditlerden korumak üzere işletmeler ve tüketicilere yönelik sektör lideri BT güvenliği yazılımları ve hizmetleri geliştiriyor. Uç nokta ve mobil güvenlikten şifreleme, çok faktörlü kimlik doğrulaması ile uç nokta algılama ve yanıt çözümlerine kadar ESET'in yüksek performanslı, kullanımı kolay ürünleri 7/24 rahatsız etmeden koruyup denetler ve önlemlerini gerçek zamanlı olarak günceller. Böylece kullanıcıları güvende tutarken şirketlerin kesintisiz faaliyet göstermesini sağlar. Gelişen tehditlere karşı teknolojinin güvenli bir şekilde kullanılmasını sağlayan bir BT güvenlik şirketine ihtiyaç vardır. Dünya çapındaki ESET AR-GE merkezleri ortak geleceğimizi desteklemek üzere bu amaca ulaşmak için çalışır. Daha fazla bilgi için bizi www.eset.com adresinde ziyaret edin veya LinkedIn, Facebook ve Twitter'da takip edin.

Katkıda Bulunan Editörler:

Rene Holt, ESET PR Yazarı
James Shepperd, ESET PR Yazarı
Branislav Ondrasik, ESET Güvenlik Araştırma İletişim Müdürü

Ek Katkı sağlayanlar:
WeLiveSecurity
ESET Creative Studio


CYBERSECURITY
EXPERTS ON YOUR SIDE