TEMMUZ-EYLÜL 2023

SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

ŞEKİLLER

GİRİŞ

2023 yılının son çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda yine birbirinden ilginç konularla karşınızdayız. Bilişim sistemleri aracılığıyla hırsızlık ve dolandırıcılık gibi siber suçlar giderek artıyor. Özellikle dijitalleşmenin hızla yayılması, suçlulara yeni fırsatlar sunuyor. Bu tür suçlara hukuki bir bakış açısını içeren makalemizi sizlerin istifadesine sunuyoruz.

Devlet destekli siber saldırılar da önemli bir gündem maddesi olarak karşımıza çıkıyor. Bu raporumuzda Çin destekli bilgisayar korsanlarının Microsoft'un imza anahtarını çalmasına izin veren hataları inceliyoruz. Bu tür siber saldırıların giderek karmaşıklaştığını ve önlenmelerinin ne kadar kritik olduğunu vurguluyoruz.

Bulut teknolojileri hızla yaygınlaşıyor ve bu da yeni güvenlik zorlukları doğuruyor. Bu nedenle, bulut doğal uygulamaların güvenliğini artırmak için kullanılan platformları ve stratejileri ele alıyoruz. Aynı şekilde, uzaktan çalışma yaygınlaşırken güvenli erişim hizmetlerinin önemi de büyüyor. Bu raporda, Secure Access Service Edge (SASE) konseptini inceleyerek, organizasyonların güvenli erişimi nasıl sağlayabileceğini açıklıyoruz.

Geçici posta hizmetleri de veri güvenliği açısından hassas bir alan haline geliyor. Bu başlık altında, bu tür hizmetlerde hassas bilgilerin keşfedilmesi risklerini ve bu risklerin nasıl azaltılabileceğini ele alıyoruz.

JWT (JSON Web Token) tokenları, kimlik doğrulama ve yetkilendirme için kullanılan önemli araçlardan biridir. JWT tokenlarının işleyişini ve güvenliğini ele alarak, bu konuda bilgi sahibi olmanızı amaçlıyoruz.

Siber saldırganların klavye vuruşlarından bilgi çalma yöntemleri giderek daha sofistike hâle geliyor. Bu tür yan kanal saldırılarının nasıl çalıştığının ve bunlara karşı tedbirlerin incelenmesi raporumuzun bir diğer parçası.

Son olarak, WinRAR gibi yaygın kullanılan yazılımlardaki zafiyetlerin ciddiyetini ele alıyoruz. WinRAR'ın uzaktan kod yürütme zafiyeti CVE-2023-38831, yazılım güncellemelerinin ne kadar önemli olduğunu bir kez daha gözler önüne seriyor.

Geleneksel güvenlik modellerinin yetersiz kaldığı bir dönemde, Zero Trust modeli de önemli bir gündem maddesi olarak öne çıkıyor. Güvenliğin sadece güvenilir iç ağlarla sınırlı tutulmayıp bütün cihazlara ve kullanıcılara nasıl genişletilebileceğini göstermek için bu modeli ele alıyoruz.

Son konumuzu her raporumuzda güncellediğimiz honeypot verilerimize yer ayırdık.

İyi okumalar.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. Bulut Doğal Uygulamalar (CNAPP)

Bulut Doğal Uygulamalar (CNAPP), günümüzün hızla değişen ve gelişen yazılım geliştirme ekosistemindeki önemli bir kavramdır. Bu rapor, CNAPP'in ne olduğunu, sunduğu çözümleri, gelişim sürecini ve ekosisteme olan katkılarını ayrıntılı bir şekilde ele alacaktır. Ayrıca, CNAPP'in bir bulut ağında nasıl uygulandığını inceleyeceğiz.

CNAPP Nedir?

CNAPP, Bulut Doğal Uygulamalar olarak da adlandırılır ve modern yazılım geliştirme pratiğinin bir sonucu olarak ortaya çıkmış bir yaklaşımdır. Temel özellikleri şunlardır:

Temel Kavramlar

CNAPP, aşağıdaki temel kavramları içerir: konteynerizasyon, orkestrasyon ve mikroservis mimarisi. Konteynerizasyon, uygulamaların bağımsız ve izole konteynerlara paketlenmesini sağlar. Orkestrasyon, bu konteynerlerin otomatik olarak dağıtılmasını, ölçeklenmesini ve yönetilmesini kolaylaştırır. Mikroservis mimarisi ise büyük ve karmaşık uygulamaları daha küçük ve yönetilebilir parçalara böler.

CNAPP'in Avantajları

CNAPP modern yazılım geliştirme süreçlerinde bir dönüm noktası olarak kabul edilir ve bir dizi önemli avantaj sunar. Bu avantajlar, işletmelere projelerini daha verimli ve etkili hâle getirerek rekabet avantajı sağlar. Ayrıca uygulamaların daha hızlı bir şekilde geliştirilmesini ve dağıtılmasını mümkün kılar. İçerdiği konteyner teknolojileri sayesinde uygulamaların daha bağımsız ve taşınabilir olmasına olanak sağlar. Saydığımız anahtar noktalar sayesinde yazılım geliştirme ekipleri yeni özellikleri daha hızlı bir şekilde kullanıma sunabilirler. CNAPP, uygulamaların ihtiyaca göre otomatik olarak ölçeklenmesini de kolaylaştırır. İş yükü arttığında, yeni konteyner örnekleri hızla oluşturulabilir ve trafik artışına yanıt olarak kaynaklar artırılabilir. Bu, olay temelli sistemlerin veya büyük veri analitiği platformlarının hızlı ve dinamik ölçeklenmesi için idealdir. CNAPP güvenlik önlemlerinin kolayca uygulanmasını sağlar. Konteynerler, birbirlerinden izole şekilde çalıştıkları için bir konteynerin güvenlik ihlali teorik olarak diğerlerini etkilemeyecektir. Ayrıca, güvenlik yamaları ve güncellemeleri hızla uygulanabilecektir. Örneğin bir sağlık hizmeti sağlayıcısı, hassas hasta verileri için CNAPP kullanarak yüksek düzeyde veri güvenliği sağlayabilir. CNAPP, kaynakların etkin kullanılmasını sağlayarak maliyetleri azaltır. Konteynerler, fiziksel sunucuların ve sanal

makinelerin üzerine inşa edilir, bu da kaynakların daha iyi paylaşılmasını ve boşa harcanmamasını sağlar. Bir eğitim kurumu öğrenci sayısındaki değişikliklere hızla uyum sağlayabilen ve aynı anda binlerce öğrenciye hizmet verebilen bir online yönetim sistemini daha düşük bir işletme maliyetiyle çalıştırabilir.

CNAPP'in Gelişimi

CNAPP kavramının evrimi, yazılım geliştirme dünyasında önemli bir dönüşümü temsil eder. Bu bölümde, CNAPP'in gelişimini inceleyeceğiz.

Geleneksel Monolitik Uygulamalardan CNAPP'e

Geleneksel monolitik uygulamalar, tüm işlevselliği tek bir büyük uygulamada birleştirirken, CNAPP, mikroservis mimarilerine geçişi teşvik eder. Bu geçiş uygulama geliştirme süreçlerini daha esnek ve hızlı hale getirir. Her bir mikroservis bağımsız olarak geliştirilebilir, dağıtılabilir ve ölçeklendirilebilir.

Bulut Bilişim Teknolojilerinin Rolü

CNAPP kavramı, bulut bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte daha da güçlenmektedir. Bulut altyapısı CNAPP'in temel bir bileşeni olarak kabul edilir. Bulut altyapısı konteyner tabanlı uygulamaların hızlıca dağıtılmasına ve ölçeklendirilmesine olanak tanır. Ayrıca, bulut hizmet sağlayıcıları CNAPP'i desteklemek için özel hizmetler sunarlar.

CNAPP Ekosistem Katkıları

CNAPP, yazılım geliştirme ekosistemine çeşitli katkılarda bulunur. Bu bölümde CNAPP'in ekosisteme olan etkilerini ele alacağız.

Geliştirici Verimliliği

CNAPP, geliştiricilerin daha hızlı ve verimli çalışmasına olanak sağlar. Konteynerler geliştirme ve dağıtım süreçlerini basitleştirir ve hızlandırır. Ayrıca her bir mikroservisin bağımsız olarak geliştirilmesi ekiplerin paralel çalışmasına olanak tanır.

Yeniden Kullanılabilirlik

CNAPP, modüler bir yaklaşımı teşvik ederek kodun yeniden kullanılabilirliğini artıran bir platform yapısıdır. Her bir mikroservis farklı projelerde veya uygulamalarda yeniden kullanılabilir. Bu da geliştirme süreçlerinin daha etkili olmasını sağlar.

İnovasyon

CNAPP, bulut sağlayıcılarına ve araç geliştiricilerine yeni fırsatlar sunar. Konteyner tabanlı uygulamaların yönetimi ve hızlı dağıtımı için özel araçlar ve hizmetler geliştirilmesi daha yaratıcı ve yenilikçi çözümlerin ortaya çıkmasına olanak tanır.

CNAPP ve Bulut Ağı Uygulamaları

CNAPP bir bulut ağında nasıl uygulanır? Bu bölümde CNAPP'in bir bulut ağında kullanılma yöntemlerini inceleyeceğiz.

Konteyner Teknolojileri

CNAPP'de uygulamalar konteynerler şeklinde paketlenerek bağımsız çalışabilir hâle getirilirler ve bulut platformları üzerinde çalıştırılabilirler. Konteynerler uygulamaların taşınabilirliğini artırır ve farklı bulut sağlayıcılar arasında kolayca geçiş yapılmasını sağlar.

Orkestrasyon Araçları

Orkestrasyon araçları CNAPP uygulamalarının otomatik olarak yönetilmesini sağlar. Kubernetes en popüler orkestrasyon araçlarından biridir. Kubernetes konteynerlerin dağıtımını, ölçeklenmesini ve izlenmesini otomatikleştirir. Bu, büyük ve karmaşık uygulamaların etkili bir şekilde yönetilmesini sağlar.

Mikroservis Mimarileri

CNAPP, mikroservis mimarileriyle uyumlu olarak çalışır ve uygulamaları daha küçük ve yönetilebilir parçalara böler. Her bir mikroservis, belirli bir işlevselliği temsil eder ve bağımsız olarak dağıtılabilir. Bu sayede uygulamalar daha modüler olurken bakımları da daha kolay hâle gelir.

DevOps Süreçleri

CNAPP, geliştirme ve işletme süreçlerini birleştirerek hızlı ve güvenilir dağıtımları destekler. DevOps süreçleri yazılım geliştirme ve işletme ekiplerinin daha yakın işbirliği yapmasını sağlar. Bu da uygulamaların daha hızlı bir şekilde geliştirilmesini, test edilmesini ve dağıtılmasını mümkün kılar.

SİBER GÜVENLİK AVANTAJLARI

İzolasyon ve Konteyner Güvenliği

CNAPP, uygulamaları izole konteynerlerde çalıştırarak güvenlik açıklarını sınırlar. Her uygulama veya mikroservis, kendi konteynerinde çalışır ve izole durumdadır. Bu, bir uygulama içindeki bir güvenlik ihlalinin diğer uygulamaları etkileme olasılığını azaltır. Ayrıca, konteyner teknolojileri, güvenlik açıklarını hızlı bir şekilde saptamak ve kapsamlı izleme sağlamak için kullanılabilir.

Hızlı Güvenlik Güncellemeleri

CNAPP, güvenlik yamaları ve güncellemeleri konteynerler üzerinde hızlı ve etkili bir şekilde uygulamayı sağlar. Konteynerlerde uygulamalar bütün bağımlılıklarıyla birlikte paketlenir, bu da güncellemelerin kolayca

dağıtılmasını sağlar. Bir güvenlik açığı tespit edildiğinde, ilgili konteynerler hızla güncellenebilir ve siber saldırılara karşı hızlı bir savunma sağlanmış olur.

Hassas Veri Güvenliği

Özellikle hassas verileri işleyen organizasyonlar için siber güvenlik kritik öneme sahiptir. CNAPP verilerin daha güvenli bir şekilde saklanmasına ve işlenmesine yardımcı olur. Hassas veriler güvenlik önlemleriyle korunan konteynerlerde işlenebilir. Finansal hizmetler, sağlık hizmetleri ve kamu sektörü gibi sektörler için bu önemli bir avantajdır. Veri sızıntıları ve güvenlik ihlalleri riskini azaltır.

Güvenlik İzleme ve Denetimi

CNAPP güvenlik izleme ve denetimini kolaylaştırır. Konteyner tabanlı uygulamaların izlenmesi ve denetlenmesi için özel araçlar ve hizmetler kullanılabilir. Bu araçlar uygulamaların güvenlik durumunu sürekli olarak izler ve anormal aktiviteleri tespit eder. Ayrıca güvenlik denetimleri daha etkili bir şekilde yapılabilir ve uyumluluk gereksinimleri karşılanabilir.

Sonuç

Cloud-Native Application Protection Protocol (CNAPP) yazılım geliştirme dünyasının dönüşümünde kritik bir rol oynamaktadır ve ayrıca siber güvenlik açısından teknik olarak güçlü bir çözümdür. İzolasyon, hızlı güvenlik güncellemeleri, hassas veri güvenliği ve güvenlik izleme gibi avantajlar, organizasyonların siber saldırılara karşı daha iyi korunmasına yardımcı olur.

2. Bilişim Sistemleri Aracılığıyla Hırsızlık ve Dolandırıcılık Suçları

Bilişim sözcüğü Türk Dil Kurumu Bilişim Terimleri sözlüğünde, "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi" olarak tanımlanmaktadır[1]. Bilişim sistemleri kavramı ise Türk Ceza Kanunu Madde Gerekçelerinde, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistem şeklinde tanımlanmaktadır[2]. Bilişim suçu, bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde kanun dışı, ahlak dışı veya yetki dışı gerçekleştirilen her türlü davranış olarak tanımlanmaktadır[3]. Bilişim suçu kavramını ifade etmek için "siber suç", "internet suçu", "bilgisayar suçu" ve "sanal suç" gibi farklı terimler de kullanılmaktadır[4].

Bilişim suçu olarak değerlendirilen ilk olayın 18 Ekim 1966 tarihinde Minneapolis *Star Tribune* gazetesinde yer alan "Bilgisayar Uzmanı Banka Hesabında Tahrifat Yapmakla Suçlanıyor" başlıklı haberde yer aldığı bilinmektedir[5]. Ülkemizde bilişim suçlarına yönelik ilk düzenleme Türk Ceza Hukukunda 1991 yılında 3756 sayılı Kanun'la yapılmıştır. Söz konusu kanun;

1. Sistemde yer alan ve sır teşkil eden bilgiyi hukuka aykırı şekilde elde edip öğrenmeyi,
2. Başkasına zarar vermek için sistemde bulunan bilgileri kullanmayı, aktarmayı ve çoğaltmayı,
3. Başkasına zarar vermek veya kendisine yarar sağlamak amacıyla sistemi ve unsurlarını tahrip etmeyi, değiştirmeyi, silmeyi ve sistemin işlemesine engel olmayı, yanlış bir şekilde işlemesini sağlamayı,
4. Sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamayı, dolandırıcılığı ve
5. Sistemi kullanarak sahtecilik yapmayı bilişim suçları içinde ele almaktadır[6].

TCK'da bilişim suçları; "Doğrudan Bilişim Suçları (Gerçek Bilişim Suçları)" ve "Dolayısıyla Bilişim Suçları" (Bilişim Bağlantılı Suçlar) olarak iki şekilde sınıflandırılmaktadır[7]. TCK'nın "Bilişim Alanında Suçlar" başlığı altında yer alan 243, 244, 245 ve 246. maddeleri "doğrudan bilişim suçları"nı içermektedir. Bilişim sistemleri aracılığıyla işlenen suçlar ise "dolayısıyla bilişim suçları" olarak tanımlanmaktadır. TCK'nın 10. bölümünde "Malvarlığına Karşı Suçlar" başlığında yer alan "nitelikli hırsızlık" ve "nitelikli dolandırıcılık" suçları da bilişim sistemleri aracılığıyla işlenen suçlardan bazılarıdır.

Bilişim Sistemleri Aracılığıyla Hırsızlık Suçu

Hırsızlık suçunun malvarlığına karşı işlenen suçların en başta geleni ve en eskisi olduğu bilinmektedir. Bu eylem sonucunda mağdurun malvarlığında eksilme olurken, fail kendisi veya başkası lehine haksız zenginleşme sağlamaktadır[8]. Hırsızlık suçu, TCK'nın 142. maddesinde "Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir" ifadesiyle yer almaktadır. Bu suçun bilişim sistemleri aracılığıyla işlenmesi nitelikli hâl olarak değerlendirilmekte ve TCK 142/2-e'de belirtildiği üzere cezası artmaktadır[1]. Burada bilişim sistemi yalnızca bir araç olarak kullanılmakta, sistemin kendisine yönelik bir zarar bulunmamaktadır.

1 Madde 142- (1) Hırsızlık suçunun; a) Kime ait olursa olsun kamu kurum ve kuruluşlarında veya ibadete ayrılmış yerlerde bulunan ya da kamu yararına veya hizmetine tahsis edilen eşya hakkında, b) (Mülga: 18/6/2014-6545/62 md.) c) Halkın yararlanmasına sunulmuş ulaşım aracı içinde veya bunların belli varış veya kalkış yerlerinde bulunan eşya hakkında, d) Bir afet veya genel bir felaketin meydana getirebileceği zararları önlemek veya hafifletmek maksadıyla hazırlanan eşya hakkında, e) Adet veya tahsis veya kullanımları gereği açıkta bırakılmış eşya hakkında, f) (Mülga: 2/7/2012-6352/82 md.) İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur. (53) (2) Suçun; a) Kişinin malını koruyamayacak durumda olmasından veya ölmesinden yararlanarak, b) Elde veya üstte taşınan eşyayı çekip almak suretiyle ya da özel beceriyle, c) Doğal bir afetin veya sosyal olayların meydana getirdiği korku veya kargaşadan yararlanarak, d) Haksız yere elde bulundurulan veya taklit anahtarla ya da diğer bir aletle kilit açmak veya kilitlenmesini engellemek suretiyle,(53) e) Bilişim sistemlerinin kullanılması suretiyle, f) Tanınmamak için tedbir alarak veya yetkisi olmadığı halde resmi sıfat takınarak, g) (…)(53) büyük veya küçük baş hayvan hakkında,(53) h) (Ek: 18/6/2014-6545/62 md.) Herkesin girebileceği bir yerde bırakılmakla birlikte kilitlenmek suretiyle ya da bina veya eklentileri içinde muhafaza altına alınmış olan eşya hakkında, İşlenmesi hâlinde, beş yıldan on yıla kadar hapis cezasına hükmolunur.

Bilişim sistemleri aracılığıyla hırsızlık konusunda farklı görüşler bulunmaktadır. TCK'nın 141. maddesinde düzenlenen hırsızlık suçunun somut nesnelerin çalınmasına yönelik olduğu, ancak bilişim yoluyla yapılan hırsızlıkta somut bir nesne çalınmadığı görüşü bunlardan biridir. Karşıt bir görüşte ise bilişim sistemleri kullanılarak somut nesnelerin de çalınabileceği belirtilmiştir. "Örneğin bir binanın güvenlik sisteminin ayrı bir bilişim sistemine bağlı olarak çalıştığı durumlarda, bilişim sistemine hukuka aykırı bir şekilde girilerek güvenlik sisteminin devre dışı bırakılması ve bu suretle binadan taşınır malların çalınması hâlinde hırsızlık suçunun bilişim sistemleri yoluyla işlendiği kabul edilmektedir." Bir diğer görüş ise bilişim sistemleri aracılığıyla failin, mağdurun hesabından kendisine para aktarması durumunda bu paranın veri olarak değerlendirilmesi ve TCK 244/4'e göre değerlendirilmesi gerekliliğidir. Ancak burada mağdurun parasının çalındığı ve malvarlığına zarar verildiği, bu nedenle de başkasına ait malvarlığı elde edildiği için nitelikli hırsızlık olarak değerlendirilmesi gerektiği görüşü de mevcuttur. Bu konudaki tartışmalar Yargıtay Ceza Genel Kurulunun 17.11.2009 tarihli E:2009/11-193, K:2009/268 sayılı kararı ile son bulmuştur[9].

Bilişim Sistemleri Aracılığıyla Dolandırıcılık Suçu

TCK'da dolandırıcılık suçu 157, 158 ve 159. maddelerde düzenlenmiştir. TCK'nın 158. maddesinde dolandırıcılık suçunun basit şekli, "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beş bin güne kadar adlî para cezası verilir" ifadesiyle yer almaktadır. Bu suçun bilişim sistemleri aracılığıyla işlenmesi nitelikli hâl olarak değerlendirilmekte ve diğer ağırlaştırıcı nedenleri ile birlikte TCK 158'de düzenlenmektedir[2]. TCK 159'da ise suçun hafifletici nedeni "Daha az cezayı gerektiren hâl" olarak bulunmaktadır[3].

Dolandırıcılık suçu da hırsızlık suçu gibi malvarlığına karşı suçlardan olmakla birlikte, bu iki suç tipi "suçla korunan hukuki yarar", "suçun maddi konusu", "suçun maddi unsuru", "suç mağdurunun rızası" olmak üzere çeşitli açılardan birbirinden ayrılmaktadır[10]. Hırsızlık suçu mağdurun rızası olmaksızın gerçekleştirilirken, dolandırıcılık suçunda mağdurun iradesi hileli davranışlarla sakatlanmaktadır ve bu sayede mağdurun malvarlığı bakımından zararlı olan ve başkalarının malvarlığı bakımından yararlı olan bir tasarrufun, mağdur tarafından gerçekleştirilmesi sağlanmaktadır [11]. Dolandırıcılık suçundan söz edilebilmesi için suçun gerçek bir kişiye karşı işlenmesi, hileli davranışlarla gerçekleşmesi ve haksız kazanç sağlanması gerekmektedir. Örneğin, internetteki bir platform üzerinden bilgisayar sattığını iddia eden bir şahıs, bilgisayarı almak isteyen bir kullanıcıyla iletişime geçerek kendi hesabına para gönderilmesini sağlar ancak bilgisayarı alıcıya göndermezse, bilişim sistemini aracı kılarak haksız kazanç sağlamış olur ve TCK 158/1-f maddesi gereğince suç işlemiş olur. Sıklıkla karşılaşılan ve bilişim sistemlerinden faydalanılarak gerçekleştirilen bir diğer dolandırıcılık türü ise sosyal medya araçlarının kullanılmasıyla gerçekleştirilen dolandırıcılıktır. Kişinin kendisini Instagram, Twitter, Tiktok vb. sosyal medya platformları üzerinden farklı biri gibi tanıtarak haksız kazanç elde etmesi TCK 158/1-f kapsamına girmekte ve nitelikli dolandırıcılık olarak değerlendirilmektedir. Ancak bu eylem bir kişinin parolasının ele geçirilmesi sonucu o kişinin sosyal medya hesabı üzerinden gerçekleştirilirse, bu durumda öncelikle bilişim sistemine izinsiz girme suçu oluşacaktır (TCK 243/1).

Bilişim Sistemleri Aracılığıyla İşlenen Hırsızlık ve Dolandırıcılık Suçlarından Korunma Yöntemleri

Bilişim suçlarındaki artış göz önünde bulundurulduğunda, devletlerin, kurum ve kuruluşların alacağı önlemlere ek olarak bireylerin bilinçlendirilmesine öncelik verilmelidir. Hırsızlık, dolandırıcılık ve bilişim sistemleri aracılığıyla işlenebilecek birçok suçtan korunmak için alınacak bireysel önlemler önem arz etmektedir.

İnternette parola, kredi kartı, banka kartı vb. bilgilerin girildiği web sitelerinin geçerli SSL sertifikalarının olmasına dikkat edilmelidir. Bilgisayarların ortak kullanıldığı internet kafe vb. ortamlarda kredi/banka kartı bilgileri girilmemeli, mecburi durumlarda sanal klavye kullanılmalıdır. Aynı parola birden fazla hesap için kullanılmamalı, seçilen parolaların kolay tahmin edilebilir olmamasına özen gösterilmelidir. Parolalar açık bir şekilde yazılı olarak herhangi bir ortamda tutulmamalı ve kimseyle paylaşılmamalıdır. İki aşamalı doğrulama özelliği sunan tüm ortamlarda bu özellik devreye alınmalı, internette bankacılık işlemleri yapılırken 3D secure sistemi kullanılmalıdır. Fiziksel kart bilgileri online alışveriş işlemlerinde kullanılmamalı, bunun yerine sanal kart kullanılmalıdır. Lisanslı işletim sistemi ve uygulamalar kullanılmalı, tüm sistemlerde her zaman güvenlik güncelleştirmeleri yapılmalıdır.

2 Madde 158- (1) Dolandırıcılık suçunun; a) Dinî inanç ve duyguların istismar edilmesi suretiyle, b) Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle, c) Kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle, d) Kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle, e) Kamu kurum ve kuruluşlarının zararına olarak, f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle, h) Tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında, i) Serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle, j) Banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla, k) Sigorta bedelini almak maksadıyla, l) (Ek: 24/11/2016-6763/14 md.) Kişinin, kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle, İşlenmesi halinde, üç yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

3 Madde 159- (1) Dolandırıcılığın, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde, şikâyet üzerine, altı aydan bir yıla kadar hapis veya adlî para cezasına hükmolunur.

3. Çin Destekli Bilgisayar Korsanlarının Microsoft Saldırıları

Haziran ayında Çin destekli bilgisayar korsan grubu bir şirketin sistemlerinden kriptografik anahtar çaldığını belirtti. Bu anahtar, saldırganların birden fazla ABD devlet kurumu da dâhil olmak üzere 25 kuruluşun bulut tabanlı Outlook e-posta sistemlerine erişmesine fırsat verdi. Microsoft, kritik verileri çalan grubun anahtarı bu kadar kolay nasıl ele geçirdiği hakkında bir açıklama yapmadı. Kurumsal sistemler arasında geçiş yapmak için kullanabilmeleri de kafalarda soru işaretleri bıraktı [12]. Söz konusu şirkete yapılan saldırıyla ilgili incelemeler başlatıldı. Saldırıya olanak sağlayan birçok hata ve ihmal olduğu düşünülüyordu.

Bu tür şifreleme anahtarları, verilere ve sistemlere erişmek isteyen kullanıcıların kimliğini kanıtlayan kimlik doğrulama metotları oluşturmak için kullanılmaktadır. Microsoft, hassas anahtarları erişim açısından kontrollü bir şekilde sakladığını açıklamasında belirtti. Ancak Nisan 2021'de belirli bir sistemde çökme yaşadıktan sonra söz konusu anahtarın çalınmasına fırsat vermesine yol açtığını ispatladı [13]. Microsoft sistemlerini, imza anahtarları ve diğer hassas verileri kilitlenme dump'ları ile sonuçlanmaması için tasarlamıştır, ancak bu anahtar bir hata nedeniyle gözden kaçmıştır. Daha da kötüsü, çökme dump'larında hatalı verileri tespit etmek için oluşturulan sistemler, şifreleme anahtarını işaretlemede başarısız olmuştu. Çökme dump'ı görünüşte incelenip temizlendikten sonra, şirketin normal kurumsal ağına bağlı bir tür önceliklendirme ve inceleme alanı olan Microsoft "hata ayıklama ortamına" taşındı. Kimlik bilgilerinin eklendiğini tespit etmek için tasarlanan tarama, anahtarın verilerdeki varlığını tespit edemedi.

Nisan 2021'de gerçekleşmesinden sonra, Microsoft'un Storm-0558 olarak adlandırdığı Çin hacker grubu, Microsoft mühendisinin kurumsal hesabının güvenliğini ihlal etti. İhlal edilen hesapla saldırganlar, anahtarların depolandığı hata ayıklama ortamına rahatlıkla erişebilmektedir. Microsoft ele geçirilen hesabın kilitlenme dump'ının sızdırıldığını doğrudan gösteren logların artık elinde olmadığını söylüyor, bu aktörün anahtarı ele geçirmesine yönelik bir ön hazırlıktı. Bu ele geçirme sayesinde saldırganlar, meşru Microsoft hesabı erişimleri oluşturmaya başlayabildiler[14].

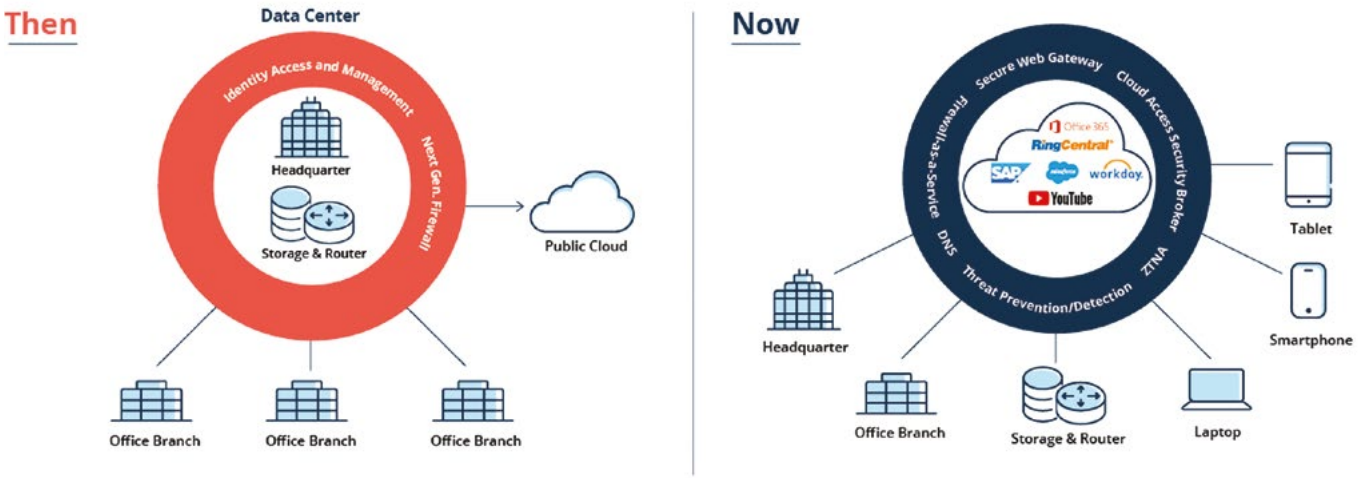
Microsoft, bu durumun şirketteki müşteri sistemlerinin imzaları kriptografik olarak doğrulamasına yardımcı olmak için sağladığı uygulama program arayüzüyle (API) ilgili bir sorundan kaynaklandığını belirtti. Durum hakkında araştırmalar devam etmektedir.

4. Secure Access Service Edge

Secure Access Service Edge'in kısaltması olan SASE değişen teknoloji altyapısıyla beraber gündeme gelmiştir. İsimlendirilmesi Gartner tarafından yapılan SASE, geleneksel ağ ve güvenlik yapısının daha bulut merkezli bir hâle gelmesinin sonucudur. Veri merkezinin firma tesislerinde bulunduğu durumlarda kullanıcılar, merkezi güvenlik cihazları üzerinden güvenlik kontrollerinden geçtikten sonra veri merkezinde bulunan uygulamalara erişmektedirler. Bulut kullanımıyla birlikte kullanıcılar ve şubeler veri merkezi sistemlerine erişmek için de internet altyapısını kullanmak zorunda kalmışlardır. Şekil 1'de bu iki mimari de gösterilmektedir. SASE de bu ihtiyaca cevap verecek şekilde kullanıcıların ve cihazların güvenli bir şekilde ağa erişimini sağlamak ve ağ trafiğini yönetmek için ortaya çıkmış bir modeldir.

SASE mimarisinin öne çıkan başlıca tarafları şunlardır:

- Ağ güvenliği politikalarının ve kurallarının merkezi bir şekilde yönetilmesini kolaylaştırır.
- Daha güvenli bir ağ erişimi sağlayarak uzaktan çalışma ihtiyacına cevap verir.
- Veri merkezi bağımlılığını azaltır ve güvenlik ürünlerini bulut üzerinden çalıştırarak gecikme sürelerini kısaltır.



Şekil 1: Geleneksel mimari ve bulut tabanlı mimari[15].

Zaman zaman iç içe geçseler de temel SASE bileşenleri ve görevleri şu şekildedir:

1. **SWG (Secure Web Gateway - Güvenli Web Ağı Geçidi):** Organizasyonların internet trafiğini güvenli bir şekilde denetlemesine ve korumasına yardımcı olur. Temel işlevleri şunlardır:
   - **Web Trafiği Filtreleme:** Kullanıcıların internet üzerinde gezinirken karşılaşabileceği zararlı yazılımlar, tehdit barındıran web siteleri vb. tehditlere karşı koruma sağlar. Bu, zararlı içerikleri ve tehlikeli bağlantılara erişimi engeller.
   - **Kullanıcı Kimlik Doğrulama:** Kullanıcıların güvenli bir şekilde internete erişmesini sağlamak için kimlik doğrulama ve yetkilendirme görevlerini üstlenir.
   - **Veri ve İçerik Denetimi:** İçerik filtrelemesi ve veri kaybı önleme (DLP) kontrolleri ile hassas verilerin izinsiz paylaşılmasını ve sızdırılmasını engeller.
2. **Güvenlik Duvarı (Firewall as a Service - FWaaS):** Tüm ağ trafiği merkezi bulut tabanlı güvenlik duvarı üzerinden yönlendirilir ve belirlenen güvenlik politikaları uygulanır. Böylece veri ve uygulamaların korunması sağlanır. Bulut tabanlı bir güvenlik hizmeti olması sayesinde ölçeklenebilirlik, esneklik ve basitleştirilmiş yönetim gibi birçok avantaj sunar.
3. **SD-WAN (Software-Defined Wide Area Networking - Yazılım Tanımlı Geniş Alan Ağı):** Ağ trafiğini yönlendirir ve verimli kullanılmasını sağlar. Temel işlevleri:
   - **Yönlendirme:** Trafik yönlendirmesini dinamik olarak sağlar. Bu durum ağ performansını artırır.
   - **Çoklu Bağlantı Yönetimi:** Birden fazla ağ bağlantısını (örneğin, MPLS, internet, 4G/5G) etkili bir şekilde yönetebilir. Çoklu bağlantı yedeklilik ve yük dengelemesi sağlar.
4. **CASB (Cloud Access Security Broker - Bulut Erişim Güvenliği Aracısı)**: Bulut uygulamalarına erişimi kontrol eden güvenlik bileşenidir. Yetenekleri şu şekildedir:
   - Bulut tabanlı uygulamalara erişimde önemli rol oynar. Bu özelliğiyle kullanıcıların uygulamalara güvenli bir şekilde bağlanmasını ve verilerini korumasını sağlar.
   - Organizasyonların bulut uygulamaları için güvenlik politikaları uygulayabilmesini sağlar. Veri koruma, kimlik doğrulama ve erişim denetimleri gibi çeşitli güvenlik özellikleri içerebilir.
   - Hassas verilerini bulut uygulamalarında korumalarına sağlar. Veri sızıntısını önlemek için DLP (Data Loss Prevention) özelliklerini içerebilir.
5. **ZTNA (Zero Trust Network Access - Sıfır Güven Ağ Erişimi):** SASE mimarisinin temelini oluşturan bir bileşendir. Temel işlevleri şunlardır:
   - Kullanıcılar ve cihazlar için kimlik doğrulama yapar ve sadece yetkilendirilmiş kullanıcıların kaynaklara erişimine izin verir.
   - Varsayılan olarak güvenmemeyi benimser. Erişim asla doğrudan verilmez, her zaman doğrulama ve yetkilendirme gereklidir.

Bu bileşenler, SASE mimarisinin anahtar unsurlarını temsil eder ve organizasyonların güvenliğini ve ağ performansını artırmak için bir araya getirilir. Bazı üreticiler güvenlik ürünlerini bahsi geçen bileşenlerin altında konumlandırırken, bazıları SASE yapısında yer alan ürünleri genişleterek daha geniş bir güvenlik yapısı sunmaktadır. SASE mimarisi için ekstra konumlandırılan ürünlerin bazıları şunlardır:

- **RBI (Remote Browser Isolation):** Web tarayıcısını izole ederek kullanıcıların tehditlere karşı korunmasını sağlar. Tarayıcı bulut tabanlı sunucularda çalışır ve sonuçlar kullanıcıya döndürülür.
- **DNS Güvenliği:** DNS filtreleme ve tehdit istihbaratı kullanarak kötü amaçlı DNS aktivitelerini önler. DNS erişim politikalarının belirlenmesini sağlar.
- **WAAP (Web Application & API Protection):** Web uygulamaları ve API'lerin güvenliğini sağlamak için kullanılan bir güvenlik ürünüdür. Klasik web uygulama güvenliği ürünlerinin yeteneklerine sahiptir. Bunun yanında API trafiği üzerinde detaylı güvenlik analizleri yapma yeteneğine sahiptir.

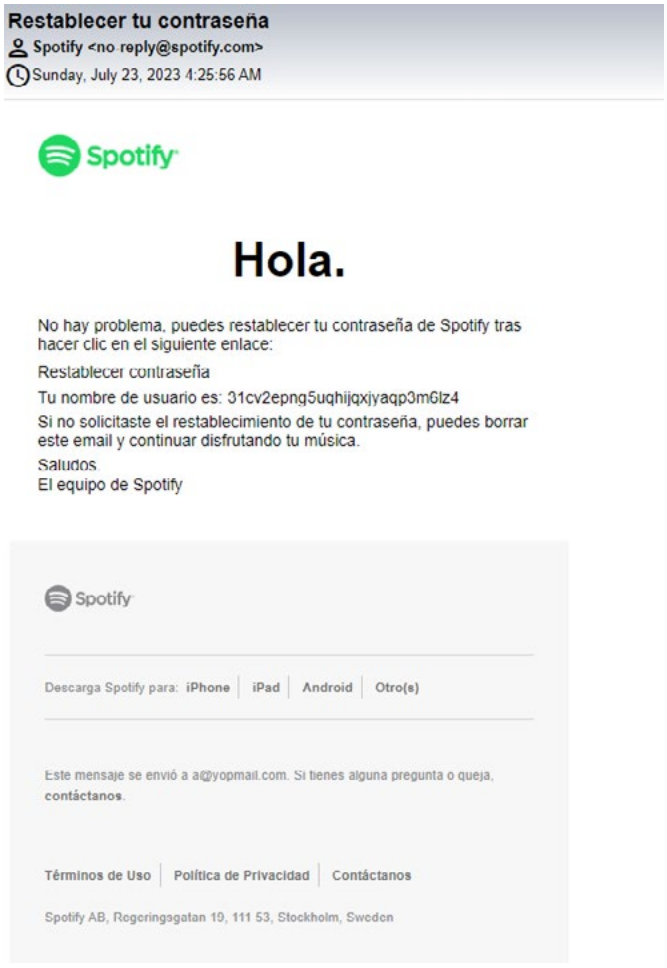
5. Geçici Posta Hizmetlerinde Hassas Bilgilerin Keşfedilmesi

Açık Kaynak İstihbaratı (Open Source Intelligence/ OSINT), belirli bir istihbarat sorusunu yanıtlamak amacıyla kamuya açık bilgilerin toplanması, değerlendirilmesi ve analiz edilmesiyle üretilen istihbarat olarak tanımlanır. Bilginin istihbarata eşit olmadığını unutmamak önemlidir. Topladığımız verilere anlam verilmeden, açık kaynaklı bulgular ham veri olarak kabul edilir. Bu bilgi ancak eleştirel düşünce zihniyetiyle bakılıp analiz edildiğinde istihbarata dönüşür [16].

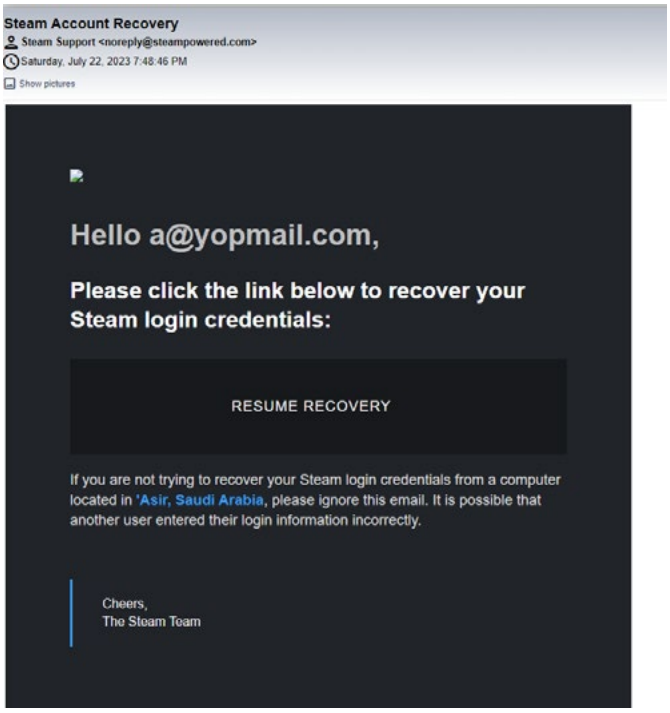
Geçici/Tek kullanımlık e-posta (temporary or disposable e-mail), belirli bir süre geçtikten sonra kendi kendini yok eden geçici bir adresten e-posta almanıza olanak tanıyan ücretsiz e-posta hizmetidir. Bunun avantajı, herhangi bir kişisel bilginin paylaşılmasına ya da kaydedilmesine gerek olmaması ve herhangi birinin adresi ele geçirmesi veya e-postanın kötüye kullanılması durumunda, adres sahibinin, diğer kişileri etkilemeden adresi kolayca iptal edebilmesidir[17]. Bazı popüler geçici/tek kullanımlık e-posta servisleri şunlardır:

- Temp Mail
- YOPmail
- TempMail+
- Dispostable - Disposable email!
- Tempr Email

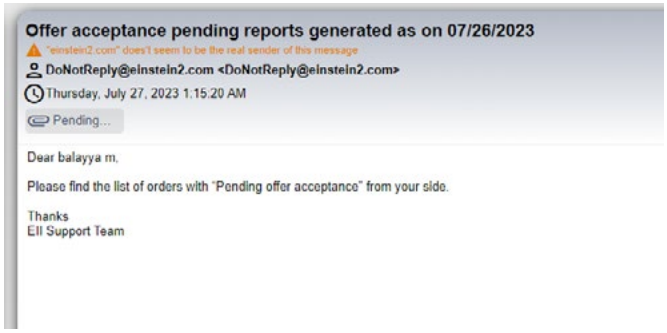
Açık Kaynak İstihbaratı, pasif ve aktif olarak ikiye ayrılır ve arama motorları, kamu kayıtları gibi çeşitli tekniklerle gerçekleştirilir. Geçici/Tek kullanımlık e-posta servislerini kullanmak da burada bir yöntemdir. Geçici/Tek kullanımlık e-posta verilerinin hizmet sunucularında barındırıldığını belirtmek gerekiyor, dolayısıyla sunucuya hizmet sağlayıcılar tarafından erişilebilir ve mevcut e-postaların gerçekte yok edilip edilmediği bilinmemektedir. Ayrıca, birçok Geçici/Tek kullanımlık e-posta hizmeti gelen kutularını herkesin erişimine açık tutarak hizmet vermektedir. Bu özellikler erişim kolaylığı sağlarken aynı zamanda önemli gizlilik ve erişim ihlallerine sebebiyet vermektedir[18]. Bazı popüler geçici/tek kullanımlık e-posta isimleri olarak şunları sayabiliriz:



Şekil 2: Geçici/Tek Kullanımlık e-posta servisinden Spotify hesabı tespit edilmesi.



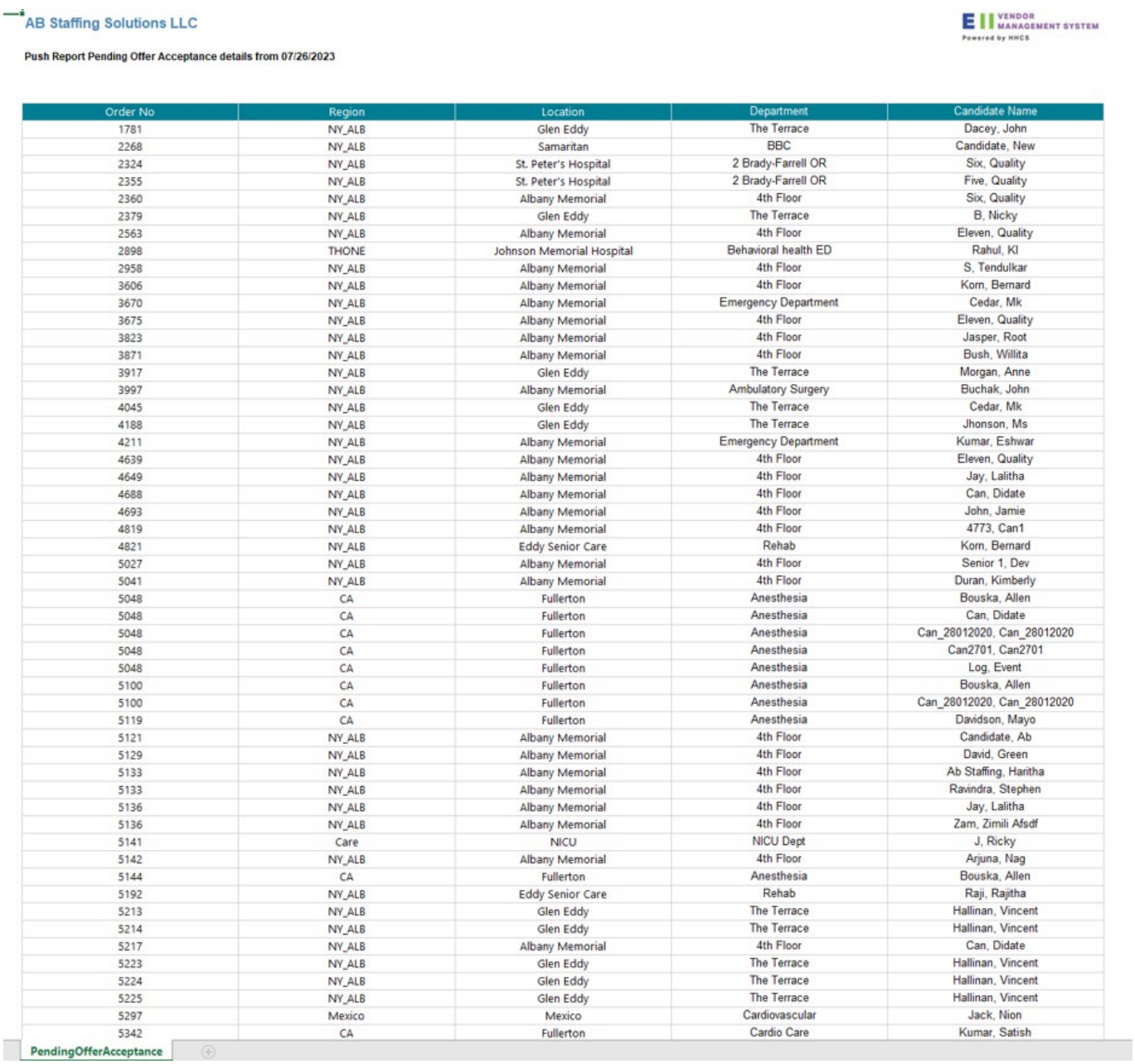
Şekil 3: Geçici/Tek Kullanımlık e-posta servisinden Steam hesabı tespit edilmesi.



Şekil 4: Geçici/Tek Kullanımlık e-posta servisinden ekinde sağlık verileri bulunan e-postanın tespit edilmesi.

- a
- aa
- aaa
- 1
- 2
- 3
- 11

Bazılarının Geçici/Tek kullanımlık e-posta servislerinin hizmetlerini; Spotify, Steam, Netflix, Facebook, Twitter, Instagram, Amazon, Aliexpress, Discord, AT&T, Grammarly, Tiktok, BTC Hesapları, kamuya açık bilgiler ve hasta kayıtları vb. gibi uygulama hesaplarını açmak için iş e-postalarına ek olarak kullandıkları tespit edilmiştir[19].



AB Staffing Solutions LLC

VENDOR MANAGEMENT SYSTEM Powered by HHCS

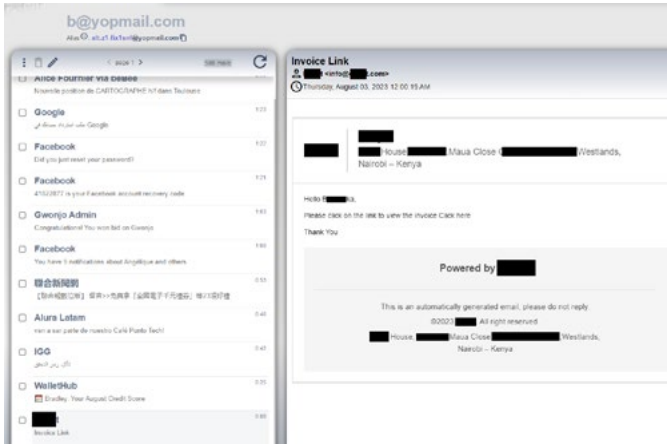
Push Report Pending Offer Acceptance details from 07/26/2023

Order No	Region	Location	Department	Candidate Name
1781	NY_ALB	Glen Eddy	The Terrace	Dacey, John
2268	NY_ALB	Samaritan	BBC	Candidate, New
2324	NY_ALB	St. Peter's Hospital	2 Brady-Farrell OR	Six, Quality
2355	NY_ALB	St. Peter's Hospital	2 Brady-Farrell OR	Five, Quality
2360	NY_ALB	Albany Memorial	4th Floor	Six, Quality
2379	NY_ALB	Glen Eddy	The Terrace	B, Nicky
2563	NY_ALB	Albany Memorial	4th Floor	Eleven, Quality
2898	THONE	Johnson Memorial Hospital	Behavioral health ED	Rahul, Kl
2958	NY_ALB	Albany Memorial	4th Floor	S, Tendulkar
3606	NY_ALB	Albany Memorial	4th Floor	Korn, Bernard
3670	NY_ALB	Albany Memorial	Emergency Department	Cedar, Mk
3675	NY_ALB	Albany Memorial	4th Floor	Eleven, Quality
3823	NY_ALB	Albany Memorial	4th Floor	Jasper, Root
3871	NY_ALB	Albany Memorial	4th Floor	Bush, Willita
3917	NY_ALB	Glen Eddy	The Terrace	Morgan, Anne
3997	NY_ALB	Albany Memorial	Ambulatory Surgery	Buchak, John
4045	NY_ALB	Glen Eddy	The Terrace	Cedar, Mk
4188	NY_ALB	Glen Eddy	The Terrace	Jhonson, Ms
4211	NY_ALB	Albany Memorial	Emergency Department	Kumar, Eshwar
4639	NY_ALB	Albany Memorial	4th Floor	Eleven, Quality
4649	NY_ALB	Albany Memorial	4th Floor	Jay, Lalitha
4688	NY_ALB	Albany Memorial	4th Floor	Can, Didate
4693	NY_ALB	Albany Memorial	4th Floor	John, Jamie
4819	NY_ALB	Albany Memorial	4th Floor	4773, Can1
4821	NY_ALB	Eddy Senior Care	Rehab	Korn, Bernard
5027	NY_ALB	Albany Memorial	4th Floor	Senior 1, Dev
5041	NY_ALB	Albany Memorial	4th Floor	Duran, Kimberly
5048	CA	Fullerton	Anesthesia	Bouska, Allen
5048	CA	Fullerton	Anesthesia	Can, Didate
5048	CA	Fullerton	Anesthesia	Can_28012020, Can_28012020
5048	CA	Fullerton	Anesthesia	Can2701, Can2701
5048	CA	Fullerton	Anesthesia	Log, Event
5100	CA	Fullerton	Anesthesia	Bouska, Allen
5100	CA	Fullerton	Anesthesia	Can_28012020, Can_28012020
5119	CA	Fullerton	Anesthesia	Davidson, Mayo
5121	NY_ALB	Albany Memorial	4th Floor	Candidate, Ab
5129	NY_ALB	Albany Memorial	4th Floor	David, Green
5133	NY_ALB	Albany Memorial	4th Floor	Ab Staffing, Haritha
5133	NY_ALB	Albany Memorial	4th Floor	Ravindra, Stephen
5136	NY_ALB	Albany Memorial	4th Floor	Jay, Lalitha
5136	NY_ALB	Albany Memorial	4th Floor	Zam, Zimili Afsdf
5141	Care	NICU	NICU Dept	J, Ricky
5142	NY_ALB	Albany Memorial	4th Floor	Arjuna, Nag
5144	CA	Fullerton	Anesthesia	Bouska, Allen
5192	NY_ALB	Eddy Senior Care	Rehab	Raji, Rajitha
5213	NY_ALB	Glen Eddy	The Terrace	Hallinan, Vincent
5214	NY_ALB	Glen Eddy	The Terrace	Hallinan, Vincent
5217	NY_ALB	Albany Memorial	4th Floor	Can, Didate
5223	NY_ALB	Glen Eddy	The Terrace	Hallinan, Vincent
5224	NY_ALB	Glen Eddy	The Terrace	Hallinan, Vincent
5225	NY_ALB	Glen Eddy	The Terrace	Hallinan, Vincent
5297	Mexico	Mexico	Cardiovascular	Jack, Nion
5342	CA	Fullerton	Cardio Care	Kumar, Satish

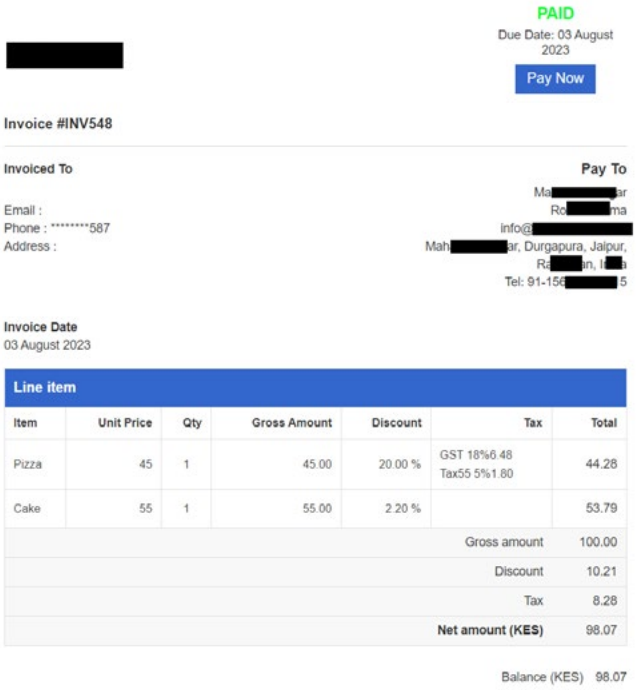
PendingOfferAcceptance

Şekil 5: Geçici/Tek kullanımlık e-posta servisinden ekinde sağlık verilerinin bulunduğu tespit edilen e-postanın Excel formatındaki içeriği.

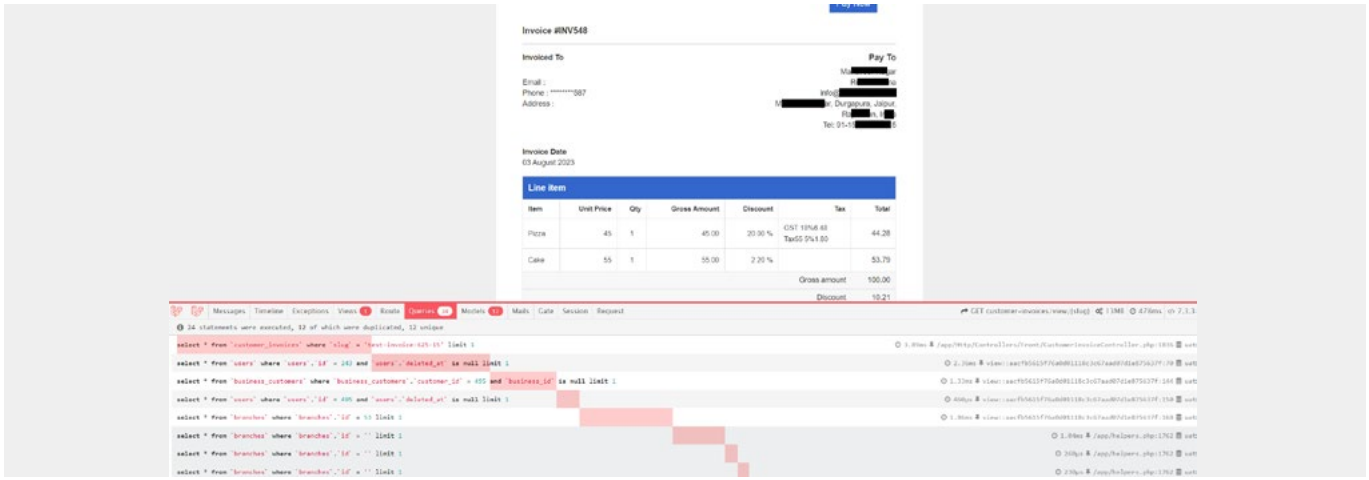
Geçici/Tek kullanımlık e-posta servisleriyle saldırganlar, Amazon AWS servisleri erişim bilgileri, Bitcoin alım satım cüzdanlarına erişim bilgileri, online alışveriş uygulamaları üzerinden ad, soyadı, kredi kartı bilgileri ve ikametgâh adresi gibi kişisel verilere erişim sağlayabilir. Erişmiş olduğu kişisel veriler ile kullanıcılara yönelik hedef odaklı oltalama (spear phishing) saldırıları gerçekleştirebilir. Akademik amaçlı gerçekleştirilen saldırı örneği; Geçici/Tek kullanımlık e-posta servisinde gerçekleştirilen çalışmalar esnasında bir e-posta adresinde fatura bilgisi tespit edilmiştir. Tespit edilen fatura bilgisinin sol butonunda bir PHP hata ayıklayıcısı simgesinin bulunduğu tespit edilmiştir. Bu sayfa incelendiğinde içerisinde önemli kimlik bilgilerinin ve bazı önemli uç noktalarının (endpoints) bulunduğu tespit edilmiştir. Tespit edilen uç noktalarından (endpoints) birisinin yönetici (admin) paneline ait olduğu belirlenmiştir. Yönetici paneli giriş sayfasına tespit edilen kimlik bilgileri ile erişim denemesi esnasında tek seferlik şifre (OTP/One Time Password) ile erişim sağlandığı tespit edilmiştir. Geçici/Tek kullanımlık e-posta servisi kullanıldığı için tek seferlik şifre (OTP/One Time Password) bu e-posta servisi mesaj kutusuna gelmiştir ve panele erişim sağlanmıştır. Yönetici sayfasında kullanıcıların listelenmesi ile uygulamayı kullanan kullanıcıların hesaplarının tamamının Geçici/Tek kullanımlık e-posta servisi ile kayıt olduğu tespit edilmiştir [20].



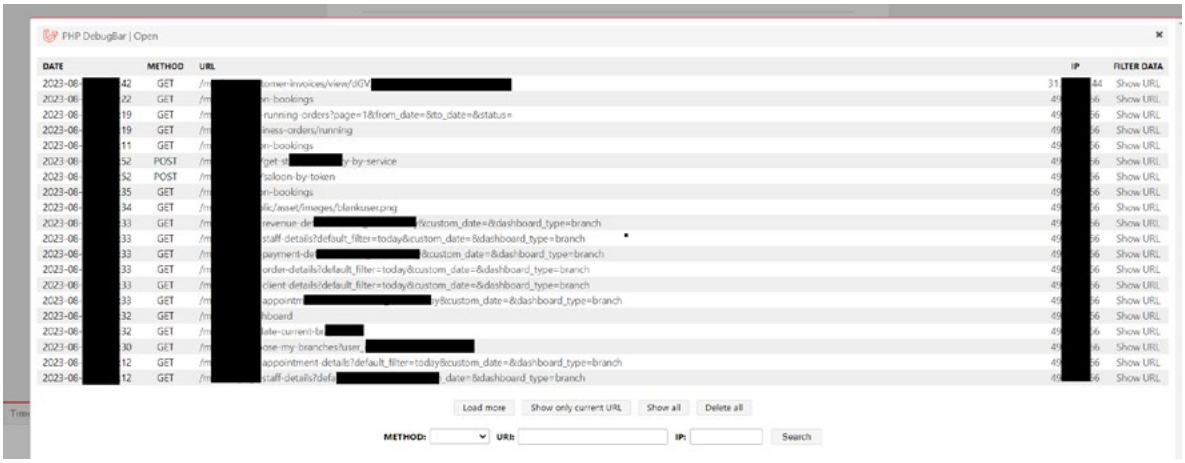
Şekil 6: Geçici/Tek kullanımlık e-posta servisinden fatura bilgisi tespit edilmesi.



Şekil 7: Tespit edilen fatura bilgisinin görüntülenmesi.

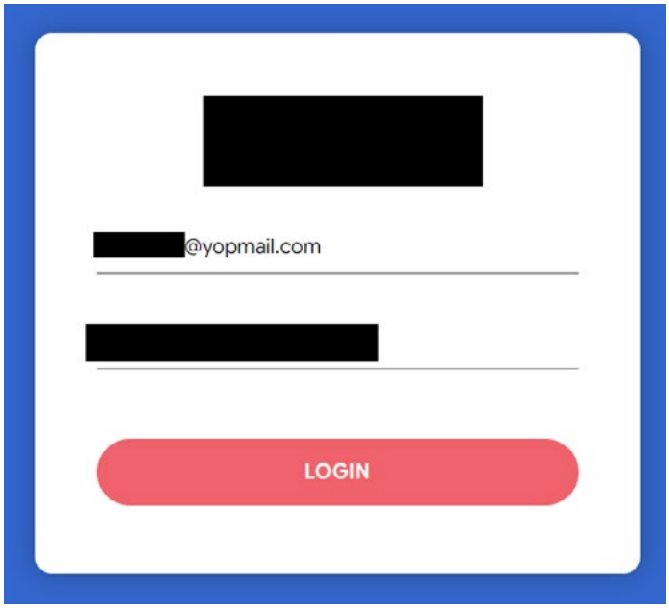


Şekil 8: Fatura bilgisi içerisindeki butonda PHP hata ayıklayıcısı bulunduğunun tespit edilmesi.

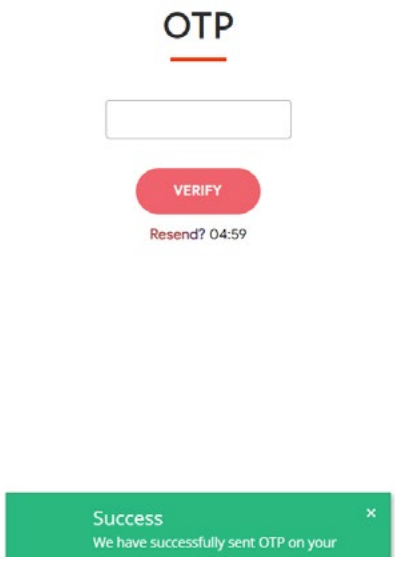


Şekil 9: Önemli uç noktalarının (endpoints) tespit edilmesi.

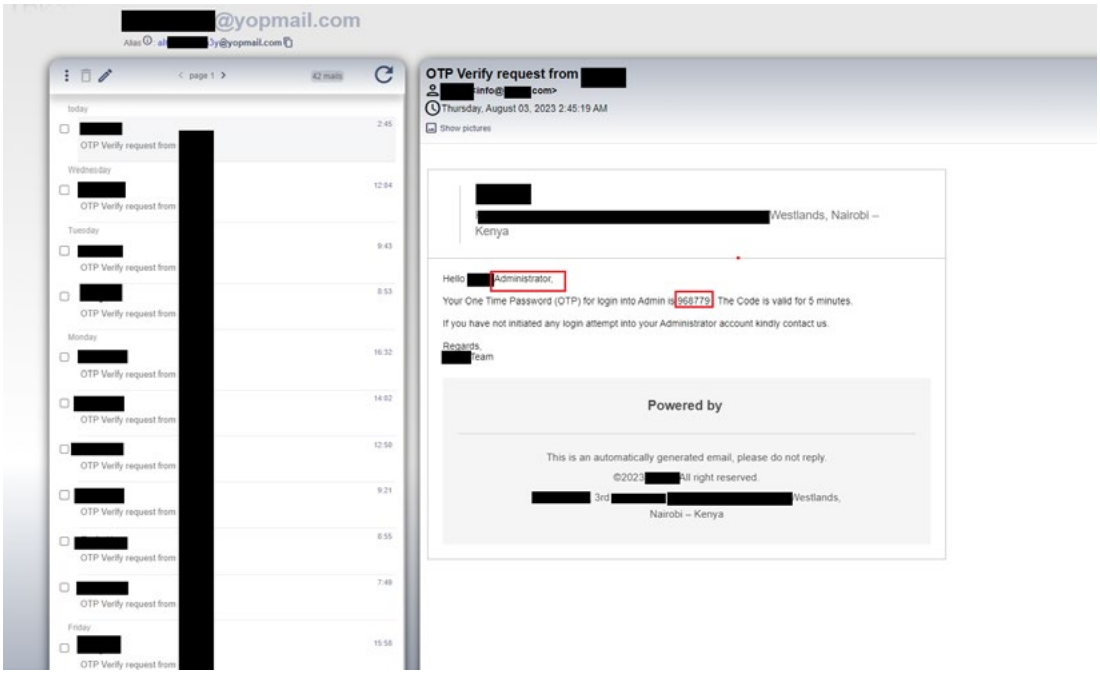
Şekil 10: Yönetici (Admin) kullanıcıya ait kimlik bilgilerinin tespit edilmesi.



Şekil 11: Yönetici sayfasına giriş denemesi.

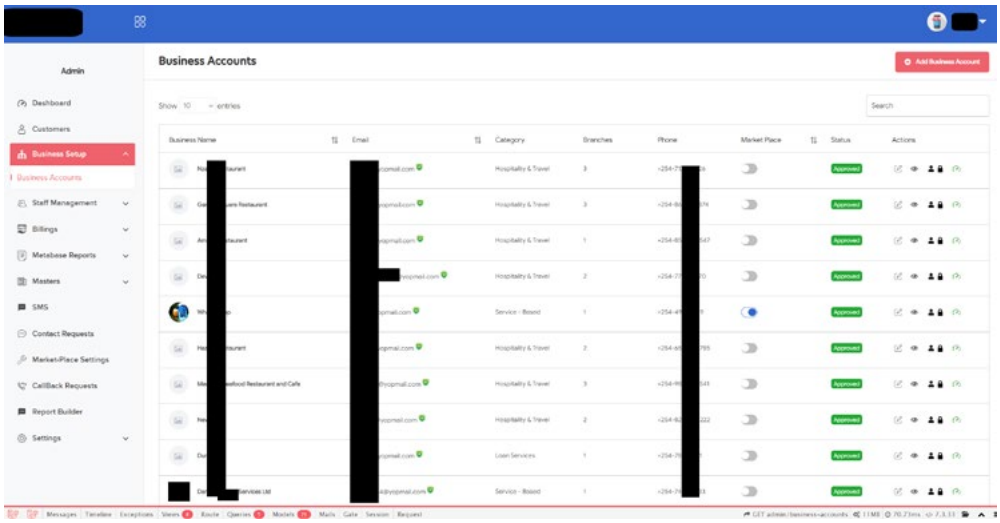


Şekil 12: Yönetici sayfasına erişim için tek seferlik şifre (OTP/One Time Password) gerekli olduğunun tespit edilmesi.



Şekil 13: Geçici/Tek kullanımlık e-posta servisinden yönetici sayfasına erişim için tek seferlik şifrenin (OTP/One Time Password) elde edilmesi.

Şekil 14: Yönetici sayfasına erişim sağlanması.



Şekil 15: Yönetici sayfasında kullanıcıların listelenmesi.

Geçici/Tek kullanımlık e-posta servislerinden bilgi toplama süreçlerini otomatik hâle getirmek için "TempMailSpy" isimli bir araç geliştirilmiştir. "TempMailSpy", Geçici/Tek kullanımlık e-posta hizmetlerinde sürekli olarak keşif yapmak ve izlemek için tasarlanmış bir Python betiğidir (script). "TempMailSpy", Telegram ve Slack API'si ile bildirim gönderebilir. Özelleştirilerek yalnızca belirli anahtar kelimelerin araması gerçekleştirilebilir [21].

```
└─# python3 defcon8.py -cf config.json -m G

The time that request has been made 2023-08-04 01:23:23

The time that request has been made 2023-08-04 01:23:23

------------------------------------------------------------

Finding Gems! - Tempmail_Plus

------------------------------------------------------------

Finding Gems! - yopMail

password Found!
Request_Time => 2023-08-03 17:37:10
Mail Title => Password changed
Mail_Sender => no-reply@spotify.com
Mail_Sender_Name =>
Mail Link: https://tempmail.plus/en/#!mail/1136482010

password Found!
Request_Time => 2023-08-03 17:36:44
Mail Title => Reset your password
Mail_Sender => no-reply@spotify.com
Mail_Sender_Name => Spotify
Mail Link: https://tempmail.plus/en/#!mail/1136481209

money Found!
Request_Time => 2023-08-03 08:45:18
Mail Title => 🚀 I N Join JustMarkets at Money Expo Mumbai 2023!
Mail_Sender => info@justmarkets.com
Mail_Sender_Name => JustMarkets
Mail Link: https://tempmail.plus/en/#!mail/1135833939

password Found!
Request_Time => 2023-08-03 08:09:16
Mail Title => Reminder: Enhance Your Account Security with a Password Reset
Mail_Sender => bounce+2e0997.9d3e8-a=mailto.plus@coins.ph
Mail_Sender_Name =>
Mail Link: https://tempmail.plus/en/#!mail/1135804880
```

Şekil 16: TempMailSpy aracı.

6. JWT Nedir?

JSON Web Token (JWT), taraflar (istemci/sunucu vb.) arasında kullanılacak olan bilgilerin JSON nesnesi olarak güvenli bir şekilde iletilmesi için kompakt ve bağımsız bir yol tanımlayan açık bir standarttır (RFC 7519). JWT içerisindeki bilgiler isteğe bağlı dijital olarak imzalanabilmekte ve bu işlem, bir gizli anahtar (secret) veya açık/gizli anahtar (public/private key) kullanılarak yapılabilmektedir[22].

JWT Yapısı

JWT Anahtarı noktalarla ayrılmış ve Base64URL ile kodlanmış karakter serileri halinde üç bölümden oluşmaktadır. Başlık (Header), Yük (Payload), İmza (Signature)[23].

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpXV
CBVeWd1bGFtYSB2ZXJpc2kiLCJpYXQiOjE1MTYy
MzkwMjJ9.8wL1fTvCkNECcYwCaT90uyk8ByoMmL
5wZjDSDmo-YoU
```

Şekil 17: Üretilmiş JWT anahtar örneği.

1. Başlık (Header)

JWT anahtarında ilk sırada bulunan başlık verisi, HMAC SHA256 veya RSA gibi kullanılacak algoritma ile anahtar tipini belirten iki farklı alandan oluşmaktadır. Örneğin, HS256 değeri HMAC-SHA256 ile şifrelendiğini gösterir.

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Şekil 18: JWT başlık (header) örneği.

2. Yük (Payload)

Anahtarı kullanacak taraflar arasında ihtiyaç duyulan verileri içeren bölümdür. Talepler (Claims) olarak belirtilen veriler üç farklı türe ayrılmıştır. Bunlar:

- Kayıtlı (registered) talepler: Zorunlu olmayan ancak kullanılması standart açısından tavsiye edilen bu talepler JWT içinde ön tanımlı olarak belirlenmiş alanları içerir. Örneğin “exp”, “sub”, “iat” vb.
- Açık (public) talepler: Kayıtlı talepler gibi ön tanımlı alanlardan oluşur ancak daha fazla değere sahiptir.
- Gizli (private) talepler: Anahtar değerini kullanacak taraflar (istemci/sunucu) arasında kullanılacak olan özel verileri içerir.

```
{
  "sub": "1234567890",
  "accessLevel": "Admin",
  "iat": 1694005973  Wed Sep 06 2023 16:12:53 GMT+0300 (GMT+03:00)
}
```

Şekil 19: JWT yük (payload) örneği.

3. İmza (Signature)

JWT anahtarının son kısmıdır. Bu kısmın oluşturulabilmesi için kodlanmış olarak başlık ve yük verisi ile birlikte uygulamaya özel bir gizli değer kullanılmalı ve imzalanmalıdır.

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  256-bit-gizli-deger
) ☐ secret base64 encoded
```

Şekil 20: HMAC SHA256 kullanılarak üretilecek imza (signature) örneği.

JWT Kullanımları ve Avantajları

JWT anahtarlarının en yaygın kullanımı, taraflar arasında yetkilendirme işlemlerinin yönetilmesidir. Günümüzde birçok yazılım çatısında JWT anahtarlarını işleyebilecek kütüphaneler bulunmaktadır. Bu kütüphaneler aracılığıyla anahtar içinde taşınan bilgilere göre uygulamaların davranışı yönetilmektedir.

Örnek bir web uygulamasına ait JWT anahtarı kullanılarak yetkilendirme işleyişi şu şekildedir:

1. Yetkilendirme için kullanıcı adı ve parola içeren form sunucuya gönderilir.
2. Sunucu üzerinde gerekli kontrol sağlandıktan sonra uygulamaya özel değer (secret) kullanılarak, istemcinin kullanacağı ek bilgileri (payload) içeren bir JWT anahtarı üretilir ve istemciye gönderilir.
3. İstemci tarafından gerçekleştirilecek olan devam işlemleri için JWT bilgisi ilgili HTTP isteklerine eklenir ve sunucuya gönderilir. Genellikle bu gönderim için isteğe ait başlık (header) bilgisine eklenen “authorization:” değeri kullanılır.

Örneğin: Authorization: Bearer <JWT Token>

4. Daha sonraki yapılan bütün HTTP isteklerinde, “Authorization” başlığı içindeki anahtar bilgisine göre sunucu elinde bulunan özel değer (secret) ile gelen JWT imzasının geçerliliğini kontrol ederek gerekli işlemi sağlar.

JWT anahtarlarının kullanımıyla sağlanan faydalar şu şekilde sıralanabilir:

1. Her bir HTTP isteğinde kullanıcı adı ve parola taşınmasına gerek kalmaz, yetkilendirme anahtar geçerliliğini yitirmediği müddetçe bu üretilen değer üzerinden gerçekleştirilir.
2. Tek bir anahtar ile birden fazla uygulama için yetkilendirme yapılabilir (örneğin, single-sign-on, aynı servisleri kullanan web ve mobil uygulamalar vb.).
3. Durumsuz (stateless) çalıştığı için herhangi bir oturum (session) yönetimine gerek yoktur. Uygulamanın çalışması için gerekli bilgiler anahtar içinde tutulur. Anahtar ise lokal hafızaya (localStorage) kaydedilerek her bir istekte buradan okunarak sunucuya gönderilir.
4. Doğrulama işlemi için klasik veritabanı veya doğrulama sunucusu gibi ek sorgular gerekmez. Bu nedenle performansı daha yüksek ve hızlıdır.

JWT Güvenliği

JWT anahtarları barındırdıkları bilgiler ve sunucu taraflı kontroller sırasında bazı güvenlik açıklarına neden olabilir. Bu nedenle yetkilendirme için JWT anahtarları kullanılırken veri doğrulama oldukça önemlidir. Kullanım sırasında dikkat edilmesi gereken bazı hususlar şöyle sıralanabilir:

1. Yetkilendirme için üretilecek olan anahtar (Access-Token) geçerlilik süresinin uzun olması durumunda, yetki değişimlerinde güvenlik açıkları oluşabilir. Bu nedenle anahtar geçerlilik süresinin kısa olması ve gerektiğinde yeniden üretilmesi için ayrı bir yenileme anahtarının (refresh Token) üretilerek taraflar arasında paylaşılması uygun olur.
2. Üretilen anahtarlardaki bilgiler istemci tarafından okunabilir. Bu nedenle geliştiriciler güvenlik açığı oluşturabilecek hassas bilgileri anahtara koymaktan kaçınmalıdır.
3. JWT anahtarına konulan bilgilerin (payload) sunucu taraflı kontrol edilmeden kullanılması güvenlik açığı oluşturabilir. Bu nedenle her istek sırasında gerekli kontrollerin tekrardan yapılması daha sıkı bir güvenlik sağlar. Bu işlem için en iyi yöntem, kontrolü sağlanacak verinin en güncel hâlini tutan bir cache mekanizmasının kullanılmasıdır.
4. JWT anahtarı oluşturulurken bir algoritma seçilmeli (alg=none kullanılmamalı), kullanılacak olan gizli anahtar değeri (secret) tahmin edilebilir ve zayıf olmamalıdır[24].
5. JWT anahtarı kullanımında “iss” değerlerinin tanımlanmış olması güvenlik kontrolü açısından önemlidir. Bu değer JWT anahtarını üreten kuruluş bilgisini içerir. Bu bilgi kullanılarak anahtar üretimi sırasında kullanılan şifreleme ve JWT anahtarının hangi hedef kaynaktan geldiği doğrulanabilir[25].

JWT Atak Örnekleri

JWT anahtarında taşınan veriler zafiyet içerecek şekilde kullanılabilir. Bu zafiyetler saldırganlar tarafından sömürülerek sistemlerin davranışı değiştirilebilir.Örnek olarak:

1. JWT anahtarları oturum durumlarını (session state) içerebilir. Bir anahtarın geçerlilik süresinin, taşıdığı oturum bilgisinden daha önce bitmemesi durumunda çağrı yapılan servisler için anahtardaki bilgiler güvenirliğini yitirmelidir. Bu bilgiler değiştirilerek saldırı gerçekleştirilebilir.
2. JWT anahtarlarını doğrulamak/yönetmek için kullanılan bazı 3. taraf uygulamaların içerdiği zafiyetler saldırganlar tarafından kullanılabilir. Bu nedenle, ilgili işlem için varsa farklı bir kütüphane kullanılabileceği gibi, ilgili kütüphanelerin zafiyet içermeyen son sürümlerinin kullanılması veya karşılaşılan zafiyete göre kullanım şeklinin düzenlenmesi gerekir. Örneğin: CVE-2022-25898 [26]
3. Saldırganlar JWT içinde bulunan özel yük (payload) değerlerini değiştirerek uygulamaların farklı davranmasını sağlayabilir. Örneğin, JWT anahtarı içinde erişim kontrolü için taşınan “isAdmin”:false değeri saldırgan tarafından “isAdmin”:true değeri ile değiştirildiğinde bu değeri kullanan alanların görünür ve kullanıma açık olması söz konusu olabilir. Böyle bir durumda, uygulamalar sadece anahtar değer içindeki veriye güvenmemeli, herhangi bir çağrı olduğunda yetki kontrolleri tekrar yapmalıdır.
4. Kullanılan 3. taraf yazılımların JWT anahtarının kullanımı için genelde birden fazla metodu vardır. Doğrulama yapılmadan kullanılan JWT anahtarları saldırganlar tarafından sömürülebilecek bir zafiyet içerir. Örneğin: Node.js içindeki “jsonwebtoken” kütüphanesi verify() ve decode() isminde iki farklı metoda sahiptir. Geliştiricilerin gelen anahtar verisini, verify() metodu ile imza ve geçerlilik kontrolü yapmadan decode() metodu ile kullanması bir güvenlik açığı içerir ve saldırganlar kendi imzaladıkları bir anahtarı kullanarak saldırı gerçekleştirebilir.
5. Başlık bilgisinde “alg”: “HS256, HS512 vb.” değeri ile imza algoritması belirlenmiş ve buna göre üretilmiş bir anahtar, saldırganlar tarafından “alg”: “none” olarak imzalanmamış bir değer olarak tekrar sunucuya gönderebilir. Bu tür durumlarda genelde sunucular güvenilir olmayan anahtar değerini reddeder ancak saldırganlar bazı karakter ayrıştırma, beklenmedik kod veya gizleme tekniklerini kullanarak bu kontrol filtrelerini atlatabilmektedir.
6. Geliştiriciler JWT anahtarı üreten kod parçasını yazarken bazen kolay tahmin edilebilir veya varsayılan değer olarak bırakılan gizli metin değerini (secret) kullanırlar. Bu tür durumlarda saldırganlar kaba zorlama (brüte-forcing) ile ilgili değeri elde edebilir ve buldukları değeri kullanarak yeni yük bilgileriyle

birlikte imzaladıkları JWT anahtar değerini sunucuya gönderebilirler.

7. Üretilen JWT anahtarlarına ait başlık bilgisi içinde "alg" parametresi zorunludur ancak başlık içinde jwk (JSON Web Key), jku (JSON Web Key Set URL) ve kid (Key ID) değerleri de bulunabilmektedir. Saldırganlar bu değerleri kullanarak kendi ürettikleri anahtar değerlerini sunucuya gönderebilir ve bu yöntemle saldırıda bulunabilmektedir [27].

7. Klavye Vuruşları Üzerinden Yapılan Yan Kanal Saldırısı

Side channel attacks (SCA), Türkçe olarak "Yan Kanal Saldırıları" olarak bilinir ve bir cihazın yaydığı sinyallerin toplanıp yorumlanmasını içerir[28]. Bu tür saldırılar, elektromanyetik (EM) dalgalar[29], güç tüketimi[30], mobil sensörler[31], [32] ve ses[33] gibi birçok yayılma türünden yararlanılarak başarılı bir şekilde gerçekleştirilmiştir. Bu geniş yelpaze sonucunda hedef cihazlar da çeşitlenmiştir; etkilenen cihazlar arasında yazıcılar, Enigma makinesi ve hatta Intel x86 işlemciler dahi yer almaktadır[29]. Kablosuz klavyelerin algılanabilir ve okunabilir EM yayılımları ürettiğini gösteren bir çalışma mevcuttur. Fakat yaygın kullanılan ve yayılımı daha kolay tespit edilebilen tuş vuruşu seslerini değerlendiren saldırı yöntemlerinin daha uygulanabilir olduğu değerlendirilmektedir. Klavye kullanıcıların klavye seslerini gizleme konusunda bir çaba göstermemesi bir başka kolaylaştırıcı faktördür. Örneğin bir parola yazarken insanlar genellikle ekranlarını gizler[28,31], ancak klavye sesini gizlemek için pek bir şey yapmazlar. Bu durum klavye akustiği konusunda yeterince uyarıcı yayın yapılmamış olmasına bağlanabilir. Bununla beraber yapılan bazı araştırmalarda basılan tuşları doğru şekilde tahmin eden bazı modeller geliştirilmiş olsa da bunlar genellikle daha eski, kalın, mekanik klavyeler üzerinde yapılan saldırıları temel almaktadır. Oysa günümüzde yaygın olarak kullanılan dizüstü bilgisayarların modern klavyelerinden çok daha belirgin akustikler elde edilebilir. Klavyeler zamanla daha az belirgin hâle gelmiş olsa da akustiklerine erişilebilecek ve işlenebilecek teknoloji dramatik bir şekilde gelişmiştir. Bu gelişmeler, mikrofon teknolojisindeki ilerlemelerin sesli internet protokolü (VoIP) aramaları[34] ve akıllı saatler[35] gibi cihazların tuş vuruşu kayıtlarını toplamak için kullanılmasını içermektedir.

Derin Öğrenme (Deep Learning -DL), makine öğrenmesinin (Machine Learning -ML) birden fazla katmanlı bağlı nöronlardan oluşan bir alt dalıdır. 1960'lardan bu yana bilgisayar alanında yaygın olmasına rağmen, DL grafik işleme teknolojisindeki gelişmelerle 2010'larda büyük bir sıçrama yaşadı[36], Jeneratif Rekabetçi Ağlar'ın (Generative Adversarial Networks -GAN) ve dönüştürücülerin (transformers) icadı gibi büyük ilerlemeler kaydedildi. DL performansındaki bu artış PyTorch gibi Python paketleri modellerini çoğu cihazda çalıştırmak için gereken araçlara ücretsiz ve neredeyse evrensel erişim sağlanmasına olanak tanımaktadır. DL modelindeki gelişmelerle klavyeler üzerindeki akustik bir saldırının olasılığı giderek daha da artmaktadır. Dizüstü bilgisayarlar masaüstü bilgisayarlardan daha taşınabilir oldukları için klavye akustiğinin yakından duyulabileceği kütüphaneler, kafe ve çalışma alanları gibi halka açık alanlarda daha fazla bulunabilirler. Ayrıca, dizüstü bilgisayarlarda aynı modeller aynı klavyeye sahip olduğu için klavye yayılımları da benzerdir. Popüler bir dizüstü bilgisayarın ASCA'ya (Akustik Yan Kanal Saldırısı) duyarlı olması o modeli kullanan birçok kullanıcının büyük bir risk altında olması anlamına gelebilir.

Yukarıdaki bilgileri dikkate alan bir grup araştırmacı tam otomatik olarak gerçekleştirilebilen akustik yan kanal saldırısı tasarladılar ve bu saldırı yönteminin gündelik yaşam ortamlarında nasıl başarılı olduğunu deneylerle gösterdiler. Bu çalışmada (1) klavyeye yönelik bir ASCA saldırısında ilk kez derin öğrenme (DL) modelleri kullanılmış ve (2) tasarlanan yöntem gerçek dünya koşullarında değerlendirilmiştir.

Deneyde 16 GB belleğe ve Apple M1 Pro işlemciye sahip olan popüler bir MacBook Pro 16 inç (2021) kullanılmıştır. Bu model son dönemde kullanılan diğer modellerle aynı klavye tasarımına sahiptir ve muhtemelen gelecekteki modellerde de aynı tasarımı kullanacaktır. Telefon kayıt modu için de iPhone 13 mini kullanılmıştır. iPhone, dizüstü bilgisayarın sol tarafından 17 cm uzaklıkta katlanmış bir mikro fiber bezin üstüne konulmuştur (bakınız Şekil 21). Bezin amacı, kayıt sırasında masa titreşimini bir miktar azaltmaktır (bu kullanılan masa türüne bağlı olarak değişebilir). Kayıtlar örnek hızı 44.100 Hz ve her bir örnek için 32 bit ile stereo olarak yapılmıştır.

Zoom kayıt modu için video konferans uygulamasının dahili işlevi kullanılarak tuş vuruşları kaydedilmiştir. Zoom toplantısında yalnızca bir katılımcı vardır (kurban) ve bu kişi MacBook'un dahili mikrofonunu kullanmaktadır. Zoom'un gürültü bastırma parametresi mümkün olan minimum seviyeye ("düşük") ayarlanmış, ancak tamamen kapatılmamıştır. Tuşlara basmadan önce "Bu Bilgisayarda Kaydet" düğmesi tıklanarak ve tuş vuruşlarını kaydettikten sonra da "durdur" düğmesi tıklanarak .m4a

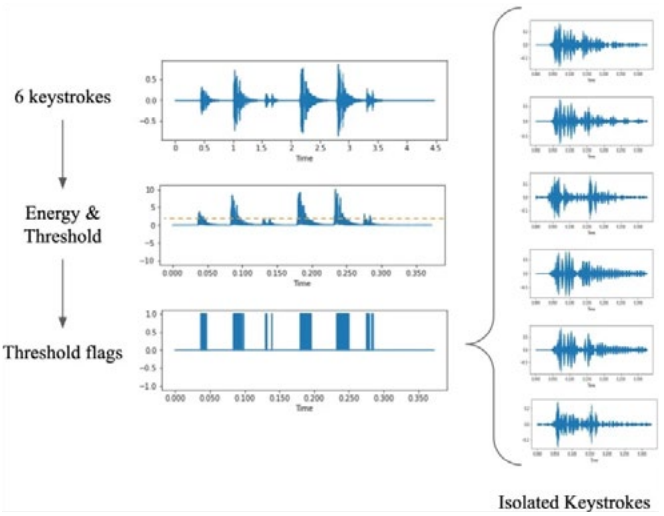
Şekil 21: Tuş vuruşlarını kaydetmek için masa kurulumu.

ses kaydı oluşturulmuş ve daha sonra .wav formatına dönüştürülmüştür.

Tüm tuş vuruşları kaydedildikten sonra bireysel tuş vuruşlarını çıkarabilen bir fonksiyona tabi tutulmuşlardır. Tuş vuruşu çıkarımı son dönem literatürünün çoğunda benzer bir yöntem olan Fourier dönüşümü ile gerçekleştirilmiş ve katsayılar frekanslar boyunca toplanarak "enerjileri" elde edilmiştir. Ardından bir enerji eşiği tanımlanarak her tuş vuruşunun varlığı belirlenmiştir. Tam izolasyon sürecinde bu veri için izole edilen tuş vuruşları sabit uzunlukta 14.400 (0.33 saniye) tutulmuştur. Fakat tuş vuruşlarını Zoom veri setiyle izole etmek daha zor olmaktadır; bunun sebebi Zoom uygulamasındaki gürültü bastırma nedeniyle tuş vuruşlarının ses seviyesinin büyük ölçüde değişmesidir, bu da bir eşik değeri belirlemenin zorluğunu artırmaktadır. Bu sorunu aşmak için araştırmacılar doğru sayıda tuş vuruşu bulunana kadar giderek daha küçük değerlerle ayarlanan bir döngü uygulamışlardır.

Araştırmacılar MacBook Pro'da 36 tuşun her birine 25 kez basmış ve her basışta üretilen sesi eğitim verisi olarak kullanmak için toplamışlardır (bakınız Şekil 22). Daha sonra her tuş için tanımlanabilir farklılıkları görselleştiren kayıtlardan dalga formları ve spektrogramlar üretilerek, tuş vuruşlarını tanımlamak için kullanılabilecek sinyalleri artırmak için belirli veri işleme adımları gerçekleştirilmiştir. Spektrogram görüntüleri bir görüntü sınıflandırıcı olan **CoAtNet** eğitim modeli kullanılarak en iyi tahminleme sonuçlarını ulaşana kadar tekrar tekrar eğitilmişlerdir. Nihai sonuçlarda CoAtNet sınıflandırıcısı akıllı telefon kayıtlarında yüzde 95, Zoom aracılığıyla yapılan kayıtlarda yüzde 93 doğruluk oranlarına ulaşmıştır. Skype uygulaması ile yapılan deneylerde daha düşük bir değer olan yüzde 91,7'lik bir doğruluk yakalansa da bu değer de başarılı bir sonuç olarak yorumlanmaktadır.

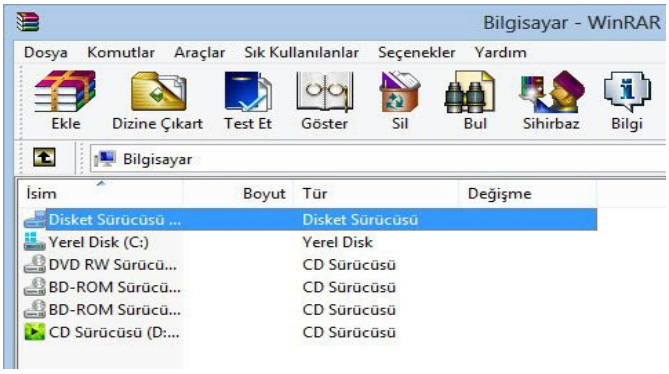
Araştırmacılar kullanıcıların bu saldırı türünden korunmak için yazma stillerini değiştirmeyi veya daha fazla karakter ve karmaşıklık içeren rasgele şifreler kullanmayı deneyebileceklerini belirtmektedir. Bunun yanı sıra potansiyel savunma yöntemleri olarak tuş vuruş seslerini beyaz gürültülerle veya yapay tuş vuruşu sesleriyle filtrelemenin de etkili olabileceğini öne sürmektedirler. Burada araştırmacılar saldırı modelinin çok sessiz bir klavyeye karşı bile son derece etkili olduğunun altına çizmektedir. Bu nedenle mekanik klavyelere ses sönümleyici eklemek veya membran tabanlı klavyelere geçmek bu saldırı modeli karşısında etkili bir savunma yöntemi olmayacaktır.



Şekil 22: Tuş vuruşu seslerinin örneklemesi.

8. WinRAR Uzaktan Kod Yürütme Zafiyeti: CVE-2023-38831

Dünya çapında milyonlarca kullanıcısı olan WinRAR en popüler sıkıştırma araçlarından biridir. Bu sebeple tehdit aktörlerinin popüler olarak kullanılan bu ve benzeri programlardaki güvenlik açıklıklarını aramak, bulmak ve sömürmek için motivasyonlarının yüksek olduğu bilinmektedir.



Şekil 23: WinRAR uygulamasından örnek bir ekran görüntüsü.

10 Temmuz 2023'te, güvenlik araştırmacıları "DarkMe" kötü amaçlı yazılımının yayılmasını araştırırken ZIP dosya formatının WinRAR tarafından işlenmesinde daha önce bilinmeyen bir güvenlik açığıyla karşılaştılar. Yaptıkları incelemelerde tehdit aktörlerinin bu programdaki bir güvenlik açığından yararlanarak "DarkMe", "GuLoader" ve "Remcos RAT" gibi çeşitli zararlı yazılımlar için taşıyıcı görevi gören ZIP arşivleri oluşturduklarını ve silah hâline getirdikleri bu arşivleri yatırım forumlarında paylaştıklarını tespit ettiler. Tehdit aktörleri kötü amaçlı yazılım sayesinde yatırımcı hesaplarından para çekebiliyorlardı. Bu güvenlik açığından Nisan 2023'ten beri faydalanıldığı tahmin edilmektedir [37].

Zafiyeti keşfeden güvenlik araştırmacıları bunu WinRAR uygulamasının sahibi olan RARLAB şirketine bildirmiştir. Bunun ardından şirket 2 Ağustos 2023 tarihinde bir güncelleme yayınlamıştır (WinRAR version 6.23). MITRE'ye bildirilen bu sıfırıncı gün zafiyeti (zero-day) CVE-2023-38831 kodunu almıştır [38].

Teknik İnceleme

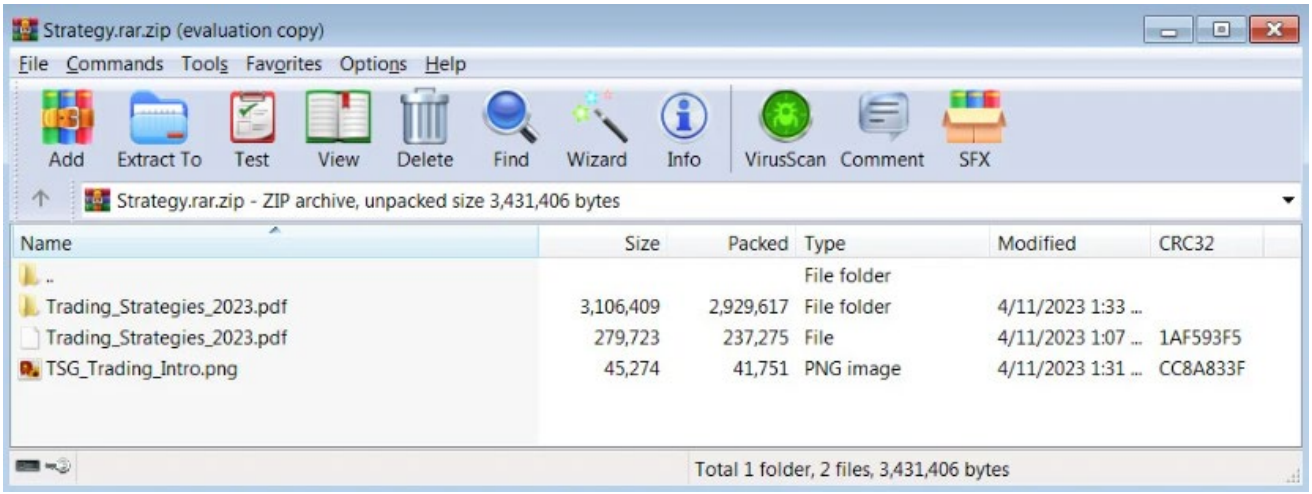
Yayınlanan raporda, kendilerini kripto para ve hisse senedi forumlarında yatırım stratejileri paylaşan yatırımcılar gibi gösteren tehdit aktörlerinin zararlı dosyaları paylaşarak bu zafiyeti sömürmeye çalıştığı tespit edilmiştir [37], [39].

Yatırım stratejileri içeriyormuş gibi görünen özel hazırlanmış forum gönderileri, PDF'ler, metin dosyaları ve resimlerden oluşuyor ve WinRAR ZIP veya RAR arşivlerine bağlantılar içeriyordu.

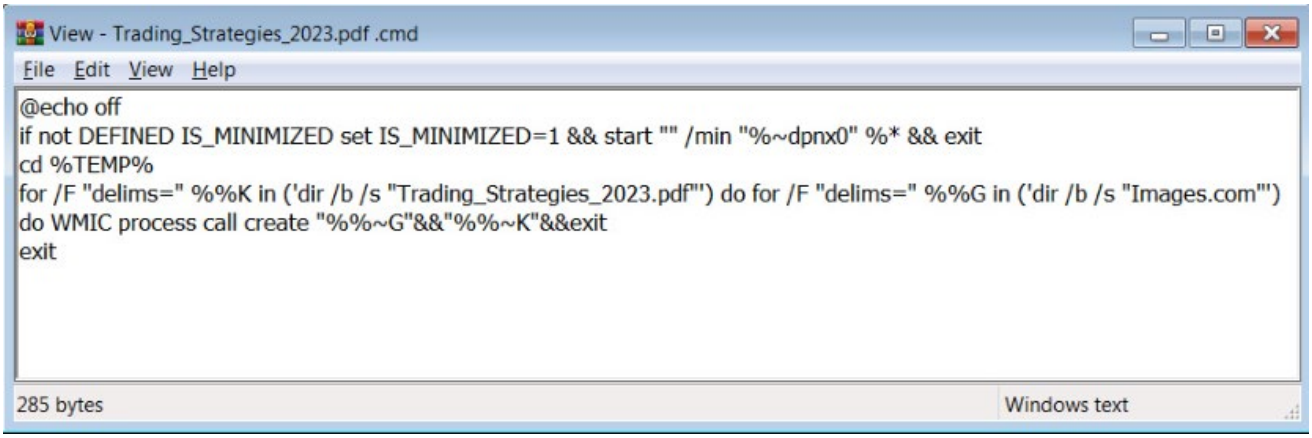
Arşivler açıldığında kullanıcılar, aşağıda gösterildiği gibi aynı dosya adıyla eşleşen bir klasöre sahip, zararsız bir PDF dosyası gibi görünen bir dosya göreceklerdir.

Ancak kullanıcı PDF'ye çift tıkladığında CVE-2023-38831 güvenlik açığından faydalanılarak, cihaza kötü amaçlı yazılım yüklemek için klasörde sessizce bir komut dosyası başlatılmaktadır. Aynı zamanda bu scriptler şüphe uyandırmamak adına tuzak belgeyi de yüklemekte ve PDF dosyası açılmaktadır.

Şekil 24: Kripto yatırım forumlarında zararlı arşiv dosyalarının paylaşılmasına ait örnek bir ekran görüntüsü.



Şekil 25: Zararlı arşiv dosyasının içeriğine bir örnek.



Şekil 26: Zafiyetin sömürülmesi esnasında çalıştırılan komut dosyası.

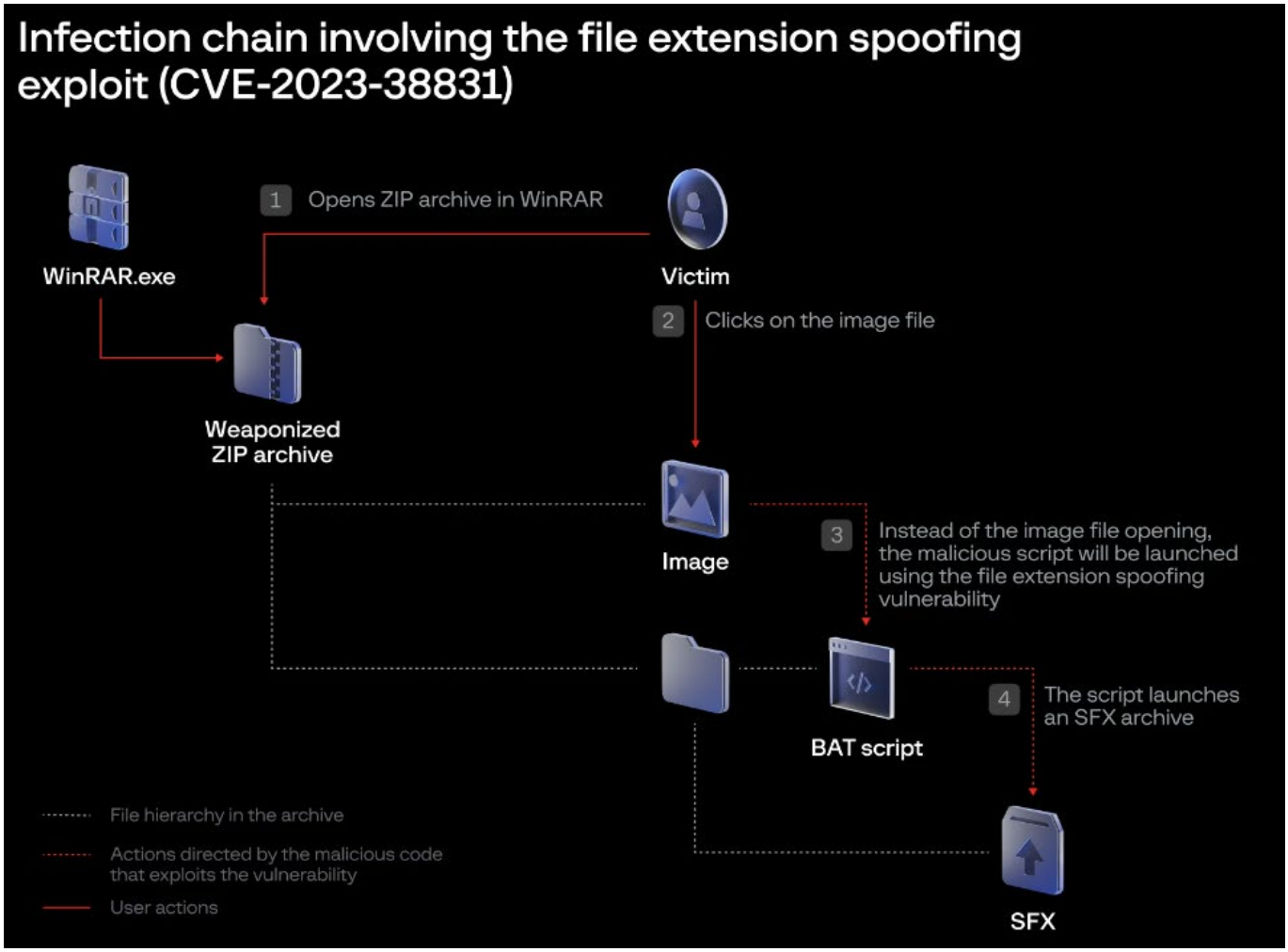
Bu güvenlik açığı normal arşiv dosyalarıyla kıyaslandığında çok az değiştirilmiş bir yapıya sahip, WinRAR'ın ShellExecute fonksiyonunun yem olarak eklenen dosyayı açmaya çalışırken yanlış parametre almasına neden olacak şekilde özel hazırlanmış arşivler oluşturulmasıyla tetiklenmektedir.

Böylece programın zararsız dosyayı atlaması ve bunun yerine toplu iş dosyasını veya CMD komut dosyasını çalıştırması sağlanır. Kullanıcı güvenli bir dosya açtığını varsayarken program farklı bir dosya başlatır.

Komut dosyası, bilgisayara "DarkMe", "GuLoader" ve "Remcos RAT" gibi çeşitli kötü amaçlı yazılımları bulaştırarak saldırgana uzaktan erişim sağlar[37], [39].

Atak şeması aşağıdaki gibidir:

WinRAR kullanıcılarına, dosya sahtekârlığı ve yakın zamanda açıklanan diğer saldırı risklerini ortadan kaldırmak için, yazılımlarını en son sürüm olan 6.23 sürümüne yükseltmeleri tavsiye edilmektedir [39].



Şekil 27: CVE-2023-38831'den faydalanan atak şeması[37].

DÖNEM KONUSU

9. Zero Trust Modeli

Sıfır güven (Zero Trust) felsefesinin temelleri, bilgisayar sistemleri için 1994 senesinde Stephen Paul Marsh'ın "Güveni bilgi işlemsel bir konsept olarak formüle etmek" (*Formalising Trust as a Computational Concept*) tezinde atılmıştır. Her ne kadar siber güvenlik çerçevesinde kullandığımız anlamdan farklı olsa da bilgisayar sistemlerinde ilk defa kullanıldığı için önemlidir. Bu tezde geçen sıfır güven (*no trust - zero trust*) kavramı, güveni hesaplama teorisi ile ilişkilidir[40].

Günümüzde ise zero trust, güvenin sürekli olarak değerlendirilmesi gerektiğini ve *implicit trust* olmaması gerektiğini savunan bir anlayıştır (içkin güven: **özneye** verilen güvenin her zaman geçerli olması; **özne** kritik bir nesneye yetkili ise diğer kritik nesnelere de yetkili olması)

Bu anlayış ilk olarak 2009 senesinde Google tarafından sunulan "beyondcorp" mimarisinde uygulanmış[41] ve ilk olarak 2010 yılında "Forrester Research" tarafından tanımlanmıştır[42].

Bugün organizasyonlar ağlarına bağlanan sayısız türde cihazla başa çıkmak zorundadır. Katı bir disiplinle sadece merkezden çalışılan, sadece kurumsal cihazların kullanılmasına izin verilen, tüm yönetim işleri organizasyon tarafından gerçekleştirilen, ağdan veri çıkışına tamamen engel olunan bir yapı kurmak mümkün olsa da birçok organizasyon için bu kurgu gerçekçi değildir. Öte yandan mevcut çözümlerle esnek çalışma ortamlarının yarattığı güvenlik problemleriyle başa çıkılması konusundaki başarısızlığa da defalarca şahit olundu. Bu sebepten ötürü kurgunun güncellenmesi kaçınılmaz hâle geldi ve "Zero Trust" modeli biçimlenmeye başladı.

Sıfır güven mimarisi, kimliği (kişi ve kişi olmayan varlıklar), kimlik bilgilerini, erişim yönetimini, işlemleri, uç noktaları, barındırma ortamlarını ve ara bağlantı altyapısını kapsayan kurumsal kaynak ve veri güvenliğine yönelik uçtan uca bir yaklaşımdır. İlk odak noktası, kaynakları erişime ihtiyacı olanlarla sınırlamak ve yalnızca görevi yerine getirmek için gereken minimum ayrıcalıkları vermeye çalışmaktır. Geleneksel mimaride organizasyonlar sınır savunmasına odaklanır ve kimlik doğrulaması yapılan kişilere, kaynaklara geniş bir yelpazede yetkili erişim hakkı verilir.

Uygulama Gereksinimleri

Zero trust modelinde tek bir kurgunun tüm organizasyonlara uymayacağını unutmamak gerekir. Organizasyonlar zero trust kurgularını kendilerine göre özelleştirmelidir. Kurgu tasarlanırken aşağıdaki unsurlar dikkate alınmalıdır.

- Altyapı karmaşıklığının uygulanabilir seviyede tutulması,
- Politika uygulamasının evrensel olarak tüm varlıklara (cihazlar, servisler vb.) ve konumlarından bağımsız olarak uygulanması,
- Çözümün kuruluş politikasına ve kamu/sektör standardına uygun, uyumlu olması,
- Eğer bulut ve fiziksel ortam kullanan bir organizasyon ise politika uygulamasının fiziksel ve bulut hibrid ortamlarında çalışması.

Hedefleri tanımlamadan önce tekrar altı çizilmesi gereken unsur sıfır güvenin bir anlayış olmasıdır. Kaynaklarda, hedefler benzer çerçevede olsa da farklılıklar gösterebilir. NIST, temel ilkelerden bahsederken harfiyen uygulanamayabilir olduğunun göz önünde bulundurulmasını belirtmektedir.

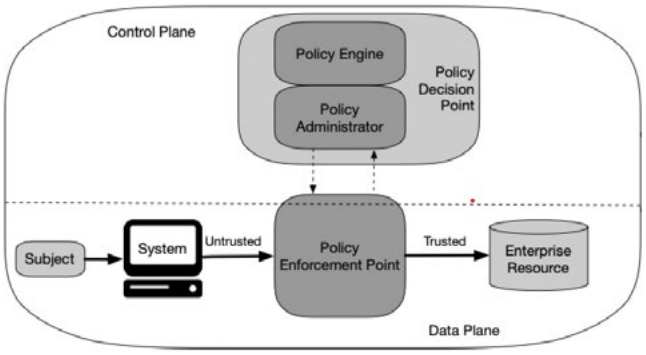
NIST 800-207 ye göre ise bu temel ilkeler aşağıdaki gibidir[43].

1. **Tüm veri kaynakları ve bilgi işlem hizmetleri kaynak olarak kabul edilmelidir:** Bir ağ birden fazla cihaz sınıfından oluşabilir. Ayrıca kişisel olarak sahip olunan cihazlar, kuruluşun sahip olduğu kaynaklara erişebiliyorsa, kişisel olarak sahip olunan cihazların da sınıflandırması yapılabilir.
2. **Ağ konumundan bağımsız olarak tüm iletişim güvence altına alınmalıdır:** Ağ konumu tek başına güven anlamına gelmez. Kuruluşun sahip olduğu ağ altyapısında bulunan varlıklardan gelen erişim istekleri, kuruluşa ait olmayan diğer ağlardan gelen erişim istekleri ve iletişim ile aynı güvenlik gereksinimlerini karşılamalıdır. Yani cihazın kurumsal ağ altyapısında bulunmasına göre güven otomatik olarak verilmemelidir. Tüm iletişim mümkün olan en güvenli şekilde yapılmalı, gizlilik ve bütünlük korunmalı ve kaynak kimlik doğrulaması sağlanmalıdır.
3. **Bireysel kurumsal kaynaklara erişim, oturum bazında verilmelidir:** Erişim izni verilmeden önce istekte bulunan kişiye olan güven değerlendirilir. Görevi tamamlamak için gereken en az ayrıcalıkla erişim sağlanmalıdır.
4. **Kaynaklara erişim, talep eden varlığın gözlemlenebilir durumu dahil olmak üzere dinamik politika tarafından belirlenmelidir:** Bir kuruluş, hangi kaynaklara sahip olduğunu, üyelerinin kimler olduğunu (veya federe bir topluluktan kullanıcıların kimliğini doğrulama yeteneğini) ve bu üyelerin ihtiyaç duyduğu kaynaklara hangi erişime sahip olduğunu tanımlayarak kaynakları korumalıdır.
5. **Kuruluş, sahip olunan ve ilişkili tüm varlıkların bütünlüğünü ve güvenlik durumunu izlemeli ve ölçmelidir:** Hiçbir varlığa işin doğası gereği güvenilmez. Organizasyon, bir kaynak talebini değerlendirirken varlığın güvenlik durumunu da değerlendirir.

6. **Tüm kaynak kimlik doğrulaması ve yetkilendirmesi dinamik olmalıdır ve erişim izni verilmeden önce sıkı bir şekilde uygulanmalıdır:** Bu, erişim elde etme, tehditleri tarama ve değerlendirme, uyum sağlama ve devam eden iletişime duyulan güveni sürekli olarak yeniden değerlendirmenin sürekli bir döngüsüdür. ZTA uygulayan bir kuruluşun Kimlik, Kimlik Bilgisi ve Erişim Yönetimi (ICAM) ve varlık yönetimi sistemlerine sahip olması beklenir. Bu, kurumsal kaynakların bir kısmına veya tamamına erişim için çok faktörlü kimlik doğrulamanın (MFA) kullanımını içerir.
7. **Organizasyon, varlıkların mevcut durumu, ağ altyapısı ve iletişimler hakkında mümkün olduğunca fazla bilgi toplamalı ve bunları güvenlik duruşunu iyileştirmek için kullanmalıdır:** Bir kuruluş, varlık güvenliği durumu, ağ trafiği ve erişim talepleri hakkında veri toplamalı, bu verileri işlemeli ve elde edilen bilgileri politika oluşturma ve uygulamayı iyileştirmek için kullanmalıdır.

Zero Trust Temel Fonksiyonları

1. **Kimlik Doğrulama ve Yetkilendirme**: Her kullanıcı ve cihaz, ağa erişim talep ettiğinde kimlik doğrulama sürecinden geçer. Bu, kullanıcıların kimliklerini belgelemesi ve yetkilendirme süreciyle hangi kaynaklara erişebileceklerinin belirlenmesi anlamına gelir.
2. **Mikrosegmentasyon**: Ağı güvenlik bölgelerine veya segmentlere bölmek, onu daha iyi yönetilebilir ve güvenli hâle getirir.
3. **Çok Faktörlü Kimlik Doğrulama (MFA)**: Çok faktörlü kimlik doğrulama, kullanıcıların kimliklerini daha güçlü bir şekilde doğrulamalarını sağlar. Bu, kullanıcıların parolalarının yanı sıra biyometrik veriler, fiziksel anahtarlar veya tek kullanımlık kodlar gibi başka bir kimlik doğrulama faktörü sunmalarını gerektirir.
4. **Erişim Kontrolleri**: Zero Trust, kullanıcıların ve cihazların hangi kaynaklara erişebileceğini sıkı bir şekilde kontrol eder. İhtiyaç duyulan en düşük düzeyde erişim yetkisi verilir ve gereksiz erişimler sınırlanır.
5. **Sürekli Gözetim ve İzleme**: Zero Trust, ağ trafiğini sürekli olarak izler ve anormal aktiviteleri tespit etmeye çalışır. Potansiyel tehditleri erken aşamada tespit etmeye yardımcı olur ve hızlı yanıt verilmesini sağlar.



Şekil 28: NIST Zero Trust Mimarisi.

Zero Trust Mimarisi (ZTA)

ZTA Bileşenleri

ZTA bileşenleri mantıksal tasarımda 2 düzeyde (plane) ele alınmaktadır. Bunlar Control Plane ve Data Plane dir.

ZTA temelde 3 bileşenden oluşmaktadır. Aşağıda bölge açıklamaları ve bileşenler anlatılmıştır.

1) Kontrol Düzeyi

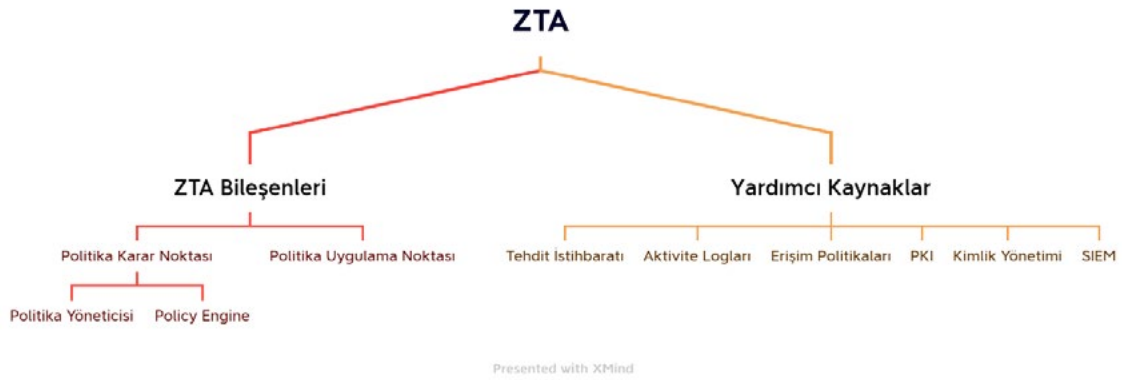
Policy Decision Point (PDP - Politika karar noktası): Kontrol düzlemi, varlıkların bakımını yapmak ve yapılandırmak için kullanılır. Ayrıca kaynak erişimi kararlarını vermek ve kaynaklar arasındaki iletişim yollarını kurma işlemleri yine kontrol bölgesinde gerçekleştirilir.

Policy Engine (PE – Politika motoru): Bu bileşen, belirli bir konu için bir kaynağa erişim izni verilmesine ilişkin nihai karardan sorumludur. PE, kaynağa erişim izni vermek, reddetmek veya iptal etmek için kurumsal politikanın yanı sıra harici kaynaklardan gelen girdileri bir güven algoritmasına girdi olarak kullanır. Politika motoru kararı verir ve günlüğe kaydeder.

Policy Administrator (PA – Politika idarecisi): Bu bileşen, bir konu ile bir kaynak arasındaki iletişim yolunun kurulmasından ve/veya kapatılmasından sorumludur.

2) Data Düzeyi: (Veri düzeyi) Uygulama verileri arasında gerçekleşen iletişim için kullanılır.

Policy Enforcement Point (PEP – Politika Tahkim Noktası): Nihai karar PEP'de verilir. Yapı olarak hem kontrol düzeyinde hem de veri düzeyinde ele alınır.



Şekil 29: ZTA bileşenleri.

Yardımcı Bileşenler

ZTA bileşenlerine ek olarak, çeşitli veri kaynakları, girdi ve politika kurallarını sağlar.

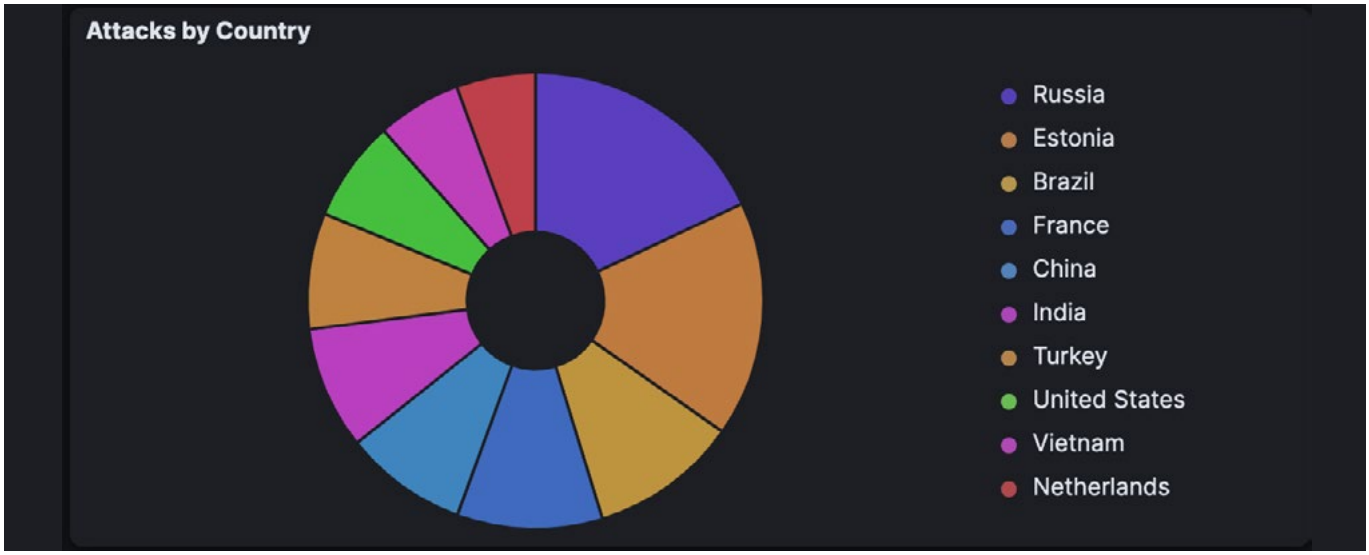
ZTA'nın etkin bir şekilde kurulması için aşağıdaki unsurlardan faydalanılabilir.

- Tehdit istihbaratı beslemeleri
- Aktivite logları
- Erişim politikaları
- PKI
- Kimlik yönetimi
- SIEM

ZTA farklı yaklaşımlar ve farklı modellerle kurulabilir. Geçiş yapmak isteyen organizasyonun kendisine uygun modeli belirleyip buna göre hareket etmesi gerekir. Bu yazıda bahsettiğimiz unsurlar birçok farklı ürün kombinasyonuyla gerçekleştirilebilir. Organizasyonların iş akışları, mevcut teknolojik altyapıları ve yatırım maliyetlerini dikkate alarak "asla güvenme, her zaman doğrula" anlayışına mümkün olduğunca uygun hareket etmesi riskleri azaltacaktır. Ancak geçiş sürecinde çok dikkatli olmak ve yanlış güvenlik algılarına kapılmamak gerekir.

Honeypot Verileri

Bu rapor son üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen kullanıcı adları ve parolalar, veriler azalan sırada listelenerek inceleme için sunulmuştur. Temmuz, Ağustos ve Eylül 2023 ayları boyunca Honeypot sensörlerimize toplam 2.297.609 saldırı gelmiştir.



Şekil 30: Gelen saldırıların ülkelere göre dağılımı.

Saldırıların Geldiği Ülke	Saldırı Sayısı
Rusya	268.082
Estonya	248.304
Brezilya	156.843
Fransa	153.161
Çin	132.119
Hindistan	130.423
Türkiye	122.512
ABD	110.166
Vietnam	88.961
Hollanda	84.415

Tablo 1: En çok saldırı gelen 10 ülke ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Rusya (yüzde 17,87) olduğu, Estonya (yüzde 16,55), Brezilya (yüzde 10,45), Fransa (yüzde 10,21) ve Çin'in (yüzde 8,9) onu takip ettiği görülmektedir. Türkiye yüzde 8,18'lik oran ile listenin 7. sırasında yer almaktadır.

Saldırılan Port	Saldırı Sayısı
445 - SMB	721.264
5900 - VNC	499.898
3389 - RDP	144.400
25 - SMTP	99.042
22 - SSH	95.051
23 - TELNET	20.184
8000 - HTTP	5.917
52869 - UPnP SOAP	5.093
8080 - TCP/HTTP	4.498
80 - HTTP	3.012

Tablo 2: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Tablo 2'de de görüldüğü üzere en çok saldırı 445 portuna gelmiştir. 445 portunda sunucuların yazıcı ve paylaşılan dosyalar için kullandığı SMB servisi çalışmaktadır. Bu yüzden SMB servisinin diğer servislerden daha çok saldırı alması beklenen bir durum olarak kabul edilebilir. SMB servisini sırasıyla VNC, RDP, SMTP, SSH ve TELNET takip etmekte. Bir önceki çeyreğe kıyasla UPnP ve web servislere yapılan saldırıların artış göstermesi dikkat çekmektedir.

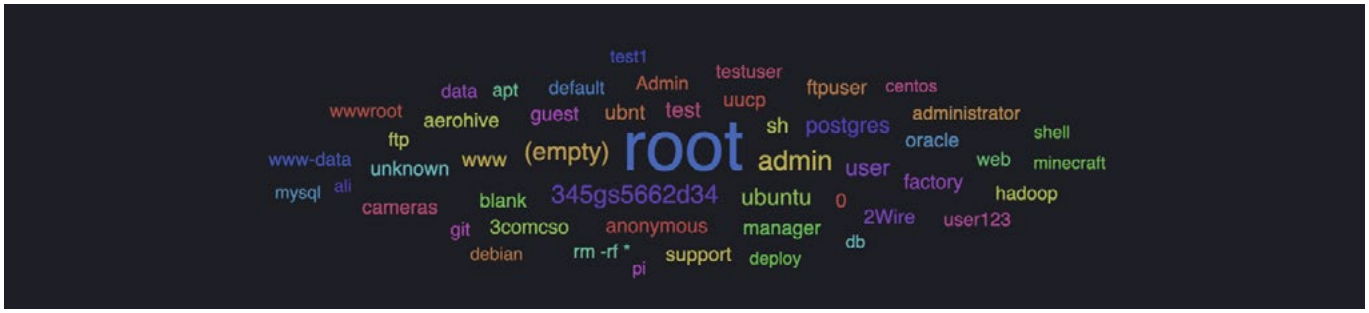
UPnP, ağ cihazlarını ve hizmetlerini keşfetmek, kurmak ve yönetmek için kullanılan bir iletişim protokolüdür. Birçok ev otomasyonu ve ağ cihazı tarafından desteklenir. Saldırganlar, UPnP ile ilgili güvenlik açıklarını hedef alarak ağa yetkisiz erişim sağlayarak çeşitli zararlı eylemlerde bulunabilir ve ağdaki cihazları tehlikeye atabilirler.

80, 8080 ve 8000 portlarında çalışan servisler genellikle web servisleri olup bu çeyrekte web uygulamalarına yönelik saldırıların arttığını söyleyebiliriz. Web uygulamalarına yapılan bu saldırılar neticesinde saldırganlar sunuculara zarar verebilir, hassas bilgileri ele geçirebilir veya hizmet kesintilerine neden olabilir.

Denenen Parola	Deneme Sayısı
123456	2.055
3245gs5662d34	1.757
345gs5662d34	1.752
admin	1.252
password	1.178
(boş)	823
123	774
12345678	647
12345	609
Password	511

Tablo 3: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

Şekil 31: Parola etiket bulutu.



Şekil 32: Kullanıcı adı etiket bulutu.

Denenen Kullanıcı Adı	Deneme Sayısı
root	64.683
admin	2.481
345gs5662d34	1.752
(boş)	1.649
ubuntu	846
user	820
postgres	640
test	552
sh	405
ubnt	343

Tablo 4: SSH ve RDP honeypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan 123456, 3245gs5662d34, admin gibi terimler gözlemlenmektedir. Bu parolaların test veya deneme süreçleri tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli ve özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için sadece sıralı sayılarla oluşturulmuş, herhangi bir harf ve özel karakter içermeyen parolalar kullanmaktan kaçınılmalıdır.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, testuser) tavsiye edilmektedir.

KAYNAKÇA

[1] "Türk Dil Kurumu Sözlükleri," 6 Mayıs 2023. [Çevrimiçi]. Available: https://sozluk.gov.tr/.

[2] "Türk Ceza Kanunu Madde Gerekçeleri," [Çevrimiçi]. Available: https://docplayer.biz.tr/1257504-Turk-ceza-kanunu-madde-gerekceleri.html. [Erişildi: 6 Mayıs 2023].

[3] "Bilişim Hukuku ve Bilişim Suçu," 6 Mayıs 2023. [Çevrimiçi]. Available: https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu.

[4] N. Gün, "Türk Ceza Hukukunda Bilişim Suçları," Ankara, 2020.

[5] M. V. Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara: Seçkin, 2020, pp. 71-72.

[6] B. Z. A. v. G. Öngören, Bilişim Hukuku,, İstanbul: Türkiye Bankalar Birliği, 2010.

[7] *Yargıtay Ceza Genel Kurulu,* 2009.

[8] Ö. Eralp, İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, İstanbul: Eralp, 2012.

[9] N. S. Agin, "Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanilmasi Suretiyle Dolandiricilik Suçu," 2019.

[10] R. Y. Yazıcıoğlu, "Hırsızlık Suçunun Malvarlığına Karşı İşlenen Bazı Benzer Suçlardan Ayrımı," *Dergipark,* pp. 757-796, 2013.

[11] F. Korkmaz, "Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi," *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* pp. 1415-1436, 2020.

[12] L. H. NEWMAN, Eylül 2023. [Çevrimiçi]. Available: https://www.wired.com/story/china-backed-hackers-steal-microsofts-signing-key-post-mortem/.

[13] 2023. [Çevrimiçi]. Available: https://www.esportsph.com/the-comedy-of-errors-that-let-china-backed-hackers-steal-microsofts-signing-key/.

[14] 2023. [Çevrimiçi]. Available: https://www.esportsph.com/the-comedy-of-errors-that-let-china-backed-hackers-steal-microsofts-signing-key/.

[15] A. Networks, "What is SASE?," [Çevrimiçi]. Available: https://www.arubanetworks.com/faq/what-is-sase/. [Erişildi: 2 10 2023].

[16] "SANS," 18 Eylül 2023. [Çevrimiçi]. Available: https://www.sans.org/blog/what-is-open-source-intelligence/.

[17] "Wikipedia," 18 Eylül 2023. [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Disposable_email_address.

[18] "DEF CON 31," 19 Eylül 2023. [Çevrimiçi]. Available: https://www.reconvillage.org/.

[19] "DEF CON 31," 19 Eylül 2023. [Çevrimiçi]. Available: https://www.youtube.com/watch?v=0Zbp-LAQZb8.

[20] "DEF CON 31," 19 Eylül 2023. [Çevrimiçi]. Available: https://www.youtube.com/watch?v=0Zbp-LAQZb8.

[21] "Github," 19 Eylül 2023. [Çevrimiçi]. Available: https://github.com/br33z3/TempMailSpy.

[22] "RFC Editor," 08 Eylül 2023. [Çevrimiçi]. Available: https://www.rfc-editor.org/rfc/rfc7519.

[23] "jwt.io," 8 Eylül 2023. [Çevrimiçi]. Available: https://jwt.io/.

[24] "wikipedia," 8 Eylül 2023. [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/JSON_Web_Token.

[25] "curity.io," 8 Eylül 2023. [Çevrimiçi]. Available: https://curity.io/resources/learn/jwt-best-practices/.

[26] "Mitre," 08 Eylül 2023. [Çevrimiçi]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25898.

[27] "portswigger.net," 8 Eylül 2023. [Çevrimiçi]. Available: https://portswigger.net/web-security/jwt#what-are-jwt-attacks.

[28] F.-X. Standaert, "Introduction to side-channel attacks," *Secure integrated circuits and systems,* pp. 27-42, 2010.

[29] Martin Vuagnoux, Sylvain Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," *USENIX security symposium,* cilt 8, pp. 1-16, 2009.

[30] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential power analysis," *Annual international cryptology conference,* pp. 388-397, 1999.

[31] Maryam Mehrnezhad, Ehsan Toreini, Siamak F Shahandashti, and Feng Hao, " Identification of user touch actions based on mobile sensors via javascript," %1 içinde *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015.

[32] Maryam Mehrnezhad, Ehsan Toreini, Siamak F Shahandashti, and Feng Hao, "Stealing pins via mobile sensors: actual risk versus user perception," %1 içinde *International Journal of Information Security*, 2018.

[33] Abubakr Abdulgadir, Richard Haeussler, Sammy Lin, Jens-Peter Kaps, and Kris Gaj, "Side-channel resistant implementations of three finalists of the nist lightweight cryptography standardization process: Elephant, tinyjambu, and xoodyak," 2022.

[34] Alberto Compagno, Mauro Conti, Daniele Lain, and Gene Tsudik, "Don't skype & type! acoustic eavesdropping in voice-over-ip," %1 içinde *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.

[35] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He, "Smartwatch-based keystroke inference attacks and context-aware protection mechanisms," %1 içinde *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016.

[36] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton, "Imagenet classification with deep convolutional neural networks," %1 içinde *Advances in neural information processing systems*, 2012.

[37] "Group-IB Threat Intelligence," 23 8 2023. [Çevrimiçi]. Available: https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/.

[38] NIST, "National Vulnerability Database," 24 8 2023. [Çevrimiçi]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-38831.

[39] B. Toulas, "BleepingComputer," 23 8 2023. [Çevrimiçi]. Available: https://www.bleepingcomputer.com/news/security/winrar-zero-day-exploited-since-april-to-hack-trading-accounts/.

[40] S. P. Marsh, "Formalising Trust as a," 1994. [Çevrimiçi]. Available: https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf. [Erişildi: 10 2023].

[41] google, "beyondcorp," 2009. [Çevrimiçi]. Available: https://www.beyondcorp.com/. [Erişildi: 02 10 2023].

[42] Forrester Research, 2010. [Çevrimiçi]. Available: https://www.forrester.com/blogs/category/zero-trust-security-framework-ztx/. [Erişildi: 02 10 2023].

[43] NIST 800-207, "https://csrc.nist.gov/pubs/sp/800/207/final," 2020. [Çevrimiçi]. Available: https://csrc.nist.gov/pubs/sp/800/207/final.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech