# Bölüm A: Savunma Mimarisi ve Teknoloji Entegrasyonu

1. AĞ VE ÇEVRE GÜVENLİĞİ (Sınır Hattı)

Firewall & IDS/IPS

Firewall kale kapısındaki muhafız gibi. "Bu IP'den gelen bu porta giremez!" der ve trafiği engeller. Sadece bildiği kötü adresleri, yasaklı portları bloklar.

IDS gözetleme kulesi. Geçen herkesi izler ama engellemez, sadece alarm verir. IPS ise aynı kule ama silahlandırılmış. Şüpheli hareketi görünce hemen bağlantıyı keser.

Neden ikisi birlikte? Saldırgan meşru bir porta (443-HTTPS) saldırı kodu gömüp gelirse, Firewall portu açık olduğu için geçirir. Ama IPS paketin içindeki zararlı kodu tespit edip durdurur.

NDR (Network Detection and Response)

Bugün trafiğin çoğu şifreli. Firewall içeriği göremez. Ayrıca saldırgan ağa girdi mi, içeride nasıl hareket ediyor?

NDR devreye girer. Şifreli trafiği deşifre etmese bile meta verilere bakar: Hangi makine hangi makineyle konuşuyor? Veri akışı ne kadar?

Örnek: Muhasebe bilgisayarı normalde sunucularla konuşmazken, aniden gece 3'te Active Directory'ye yüzlerce sorgu atmaya başladı. NDR bunu anormal bulur ve alarm üretir. Firewall sınırda durur, NDR ağın içindeki yan yayılmayı (lateral movement) yakalar.

2. UÇ NOKTA SAVUNMASI (Son Kale)

Antivirüs vs EDR

Antivirüs: Bilinen virüs listesine bakar. "Bu dosyanın hash değeri kötü mü?" Yeni saldırılara karşı kör.

EDR: Dosyaya değil davranışa bakar. "Notepad.exe neden internete bağlanıyor?" "Excel neden PowerShell çalıştırıyor?" Anormallik tespit edince süreci öldürür, makineyi izole eder.

Fileless Malware örneği: Saldırgan disk'e .exe dosyası atmıyor, direkt RAM'de PowerShell scripti çalıştırıyor. Antivirüs diskte dosya bulamaz. EDR "PowerShell şifre dosyasını okuyor ve şifreli sunucuya gönderiyor" davranışını yakalar.

Sonuç: Antivirüs ucuz ve bilinen tehditleri temizler. EDR pahalı ama modern saldırıları yakalar. İkisi birlikte kullanılır.

3. OPERASYON MERKEZİ (Beyin Takımı)

SOC & SIEM

Firewall, IPS, NDR, EDR... hepsi kendi alanında alarm üretiyor. Bu binlerce log'u kim analiz edecek?

SIEM tüm logları bir araya getirir ve korelasyon yapar:

- 09:00 - Çalışan phishing mailine tıkladı
- 09:05 - Laptop kötü IP'ye bağlandı
- 09:10 - Laptop'ta zararlı süreç başladı
- 09:15 - Laptop Active Directory'ye tarama yaptı

SIEM bu olayları birleştirip SOC analistine sunar: "Phishing → Zararlı Bağlantı → Lateral Movement tespit edildi!" Analist dashboard'da hangi cihazın şüpheli olduğunu görür ve müdahale eder.

SOAR

Sorun: Günde 500 alarm, ekip sadece 50'sini inceleyebiliyor.

SOAR playbook'larla otomatik karşılık verir. "Phishing tespit edilirse → Göndereni engelle, kullanıcıları uyar, ekin hash'ini tüm EDR'lere dağıt."

Örnek: 50 kişiye phishing maili geldi. SOAR 30 saniyede:

1. Gönderen IP'yi Firewall'da bloklar
2. 50 mailin hepsini siler
3. Kullanıcıları uyarır
4. Tıklayan varsa laptopları izole eder

İnsan müdahalesi yok, sadece rapor gönderir.

4. GENİŞLETİLMİŞ HİZMETLER (Büyük Resim)

XDR

Sorun: EDR laptopa, NDR ağa, Mail Gateway e-postaya bakıyor. Ama bunlar ayrı ekranlarda. Saldırgan multi-channel saldırı yapınca bağlantı kurmak zor.

XDR tek platformda Endpoint + Network + Email + Cloud verilerini birleştirir.

Örnek: Phishing maili (Mail logu) → Laptop link açtı (EDR logu) → OneDrive'a yükleme (Cloud logu) → Sunucuya bağlantı (NDR logu). XDR tek timeline'da gösterir ve tek komutla her cephede müdahale eder (laptop izole, IP blok, cloud erişim iptal).

MDR

Sorun: SIEM ve EDR kurduk ama 7/24 izleyecek SOC analistimiz yok.

MDR bir güvenlik firması bizim altyapıyı uzaktan izler. Onların SOC ekibi alarmları okuyup müdahale eder.

Örnek: Gece 02:00 saldırı başladı. Bizim ekip uyuyor. MDR sağlayıcısının İngiltere ofisindeki analist laptopları izole etti, sabah rapor gönderdi. İnsan kaynak eksikliğini doldurur.

SONUÇ

Her teknoloji farklı katmanda savunma yapar:

- Firewall/IPS → Sınırda, kurala dayalı
- NDR → Ağ içinde, davranış tabanlı
- EDR → Cihazda, süreç bazlı
- SIEM/SOC → Merkezi analiz
- SOAR → Otomasyon
- XDR → Bütünleşik görünürlük
- MDR → İnsan uzmanlığı

## Bölüm B: Teknik Sözlük ve Kavram Avı

1. TEMEL YAPITAŞLARI VE AĞ

Transistör & Bilgisayar

Transistör elektrik akımını açıp kapatan küçük bir anahtardır; milyarlarca transistörün saniyede milyonlarca kez açılıp kapanması (0 ve 1'ler) sayesinde bilgisayarınızda video izleyebilir, oyun oynayabilirsiniz. Yani aslında en karmaşık yazılım bile, en temelde sadece çok hızlı açılıp kapanan anahtarların kombinasyonudur.

OSI vs TCP/IP

OSI modeli 7 katmanlı ideal bir harita gibidir ama kimse günlük hayatta bu haritayı birebir kullanmaz; TCP/IP ise gerçek dünyanın 4 katmanlı pratik yol tarifidir ve internetin her noktasında bu kullanılır. OSI'yi üniversitede öğrenirsiniz ama networkte sorun çözerken TCP/IP ile çalışırsınız.

Kriptografi

Veriyi şifrelemek hem "başkası okuyamasın" (gizlilik) hem de "veri yolda değiştirilmemiştir" (bütünlük) garantisi verir. Mesela bir paket şifreli geldiğinde, sadece içeriği göremezsiniz değil, aynı zamanda içeriğin orjinal olduğundan da emin olursunuz.

---

2. SALDIRI VEKTÖRLERİ

Sosyal Mühendislik & Phishing

İnsanlar şifrelerini "çok güvenli" diye karmaşık yapar ama patron gibi davranan birine telefonda söylerler; bu yüzden sistemi hacklemek yerine insanı kandırmak (sosyal mühendislik) çok daha kolaydır. Phishing mailde "banka linki" gibi görünen sahte link göndermektir, Email Spoofing ise mailin gönderen adresini sahte göstermektir (ikisi genelde birlikte kullanılır).

Malware Dünyası

Malware "kötü amaçlı yazılım" diye geçen genel bir şemsiye terimdir (virüs, trojan, worm hepsi malware'dir). Ransomware ise malware'in özel bir türüdür; dosyalarınızı şifreler ve "para ver, açayım" der.

Zero-Day

Zero-Day, yazılım şirketinin bile henüz bilmediği bir güvenlik açığıdır; yani savunma tarafının sıfır gün zamanı vardır hazırlanmaya (yama yok, imza yok, hiçbir şey yok). Saldırgan bu açığı kullanırsa, siz "neyle vurulduğunuzu" bile anlamazsınız.

---

3. SAVUNMA MEKANİZMALARI

Yama (Patch) Yönetimi

Bir güvenlik açığı (vulnerability) yazılımdaki bir hatadır; yama (patch) ise o hatayı kapatan güncelleme dosyasıdır. Yamayı yapmazsanız, açık kapıyı kilitlemeden uyumuş gibi olursunuz.

İki Faktörlü Kimlik Doğrulama (2FA)

Sadece parola kullanmak "bir kilit" demektir; biri şifreyi çalarsa içeri girer. 2FA ikinci bir kilit ekler (telefona gelen SMS, uygulama kodu); böylece saldırganın hem parolayı hem de telefonunuzu çalması gerekir ki olasılık istatistiksel olarak çok düşer.

VPN & SSL/TLS

VPN sizi görünmez yapmaz, sadece verilerinizi şifreli bir tünelden geçirir; internetteki herkes "tünelden veri geçiyor" görür ama içinde ne olduğunu göremez. SSL/TLS ise bu tünelin içindeki

ekstra bir koruma katmanıdır; web sitesi ile aranızdaki trafiği şifreler (HTTPS'teki "S" harfi buradan gelir).

---

4. STANDARTLAR VE SÜREÇLER

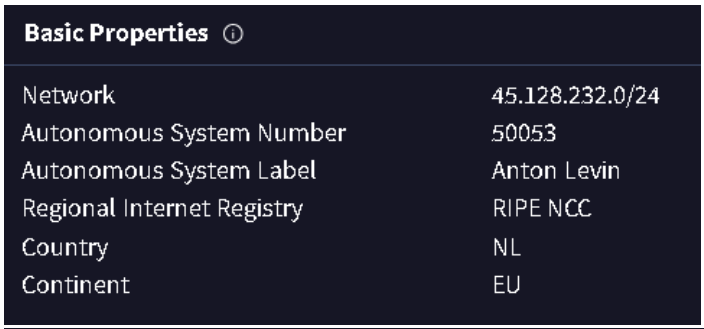
Zafiyet Taraması vs Pentest

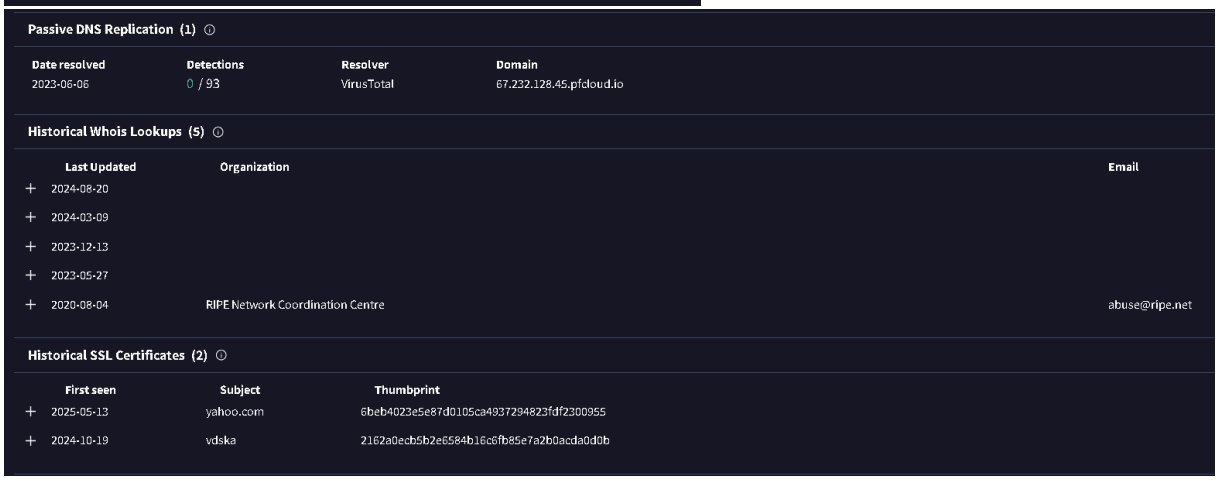
Zafiyet taraması otomatik bir robot gönderip "şu kapılar açık, şu versiyonlar eski" diye listelemektir; Pentest ise gerçek bir hackerin yapacağı gibi manuel olarak o açıklardan içeri girmeye çalışmaktır. Biri sağlık taraması, diğeri ameliyat gibidir.

Regülasyonlar (ISO 27001, NIST, GDPR)

Bu standartlar "şu güvenlik yazılımını kur" demez, "güvenliği nasıl yöneteceksin, politikan ne, sorumlular kim, kontrol nasıl yapılacak" der; yani teknik araç değil yönetim anlayışıdır. Mühendis bunları bilmeli çünkü "teknik olarak güvenli" yetmez, "kurumsal olarak yönetilebilir" olması da gerekir.

# Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi



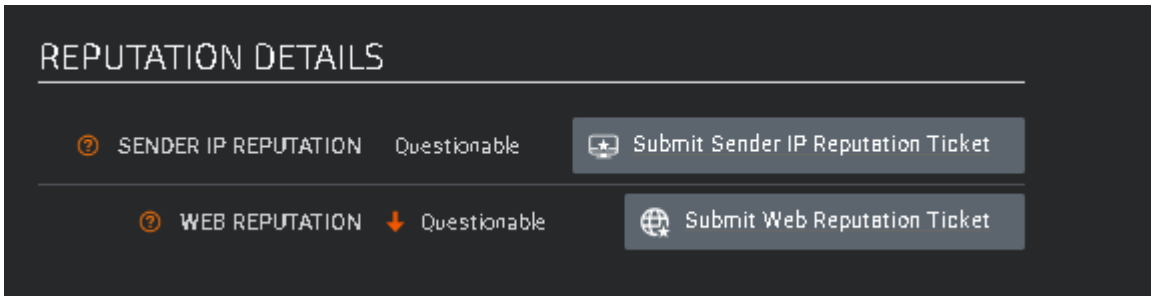



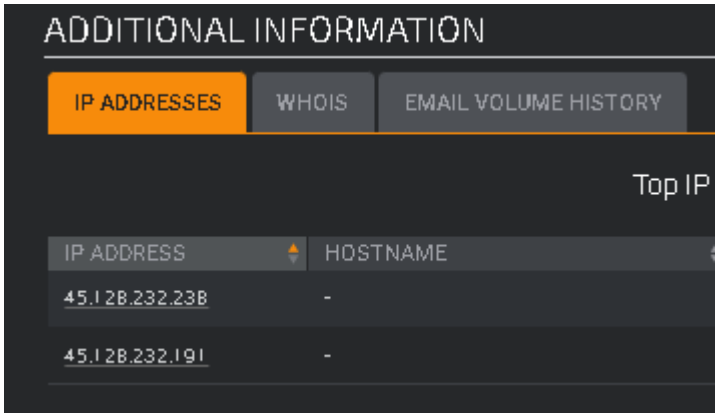


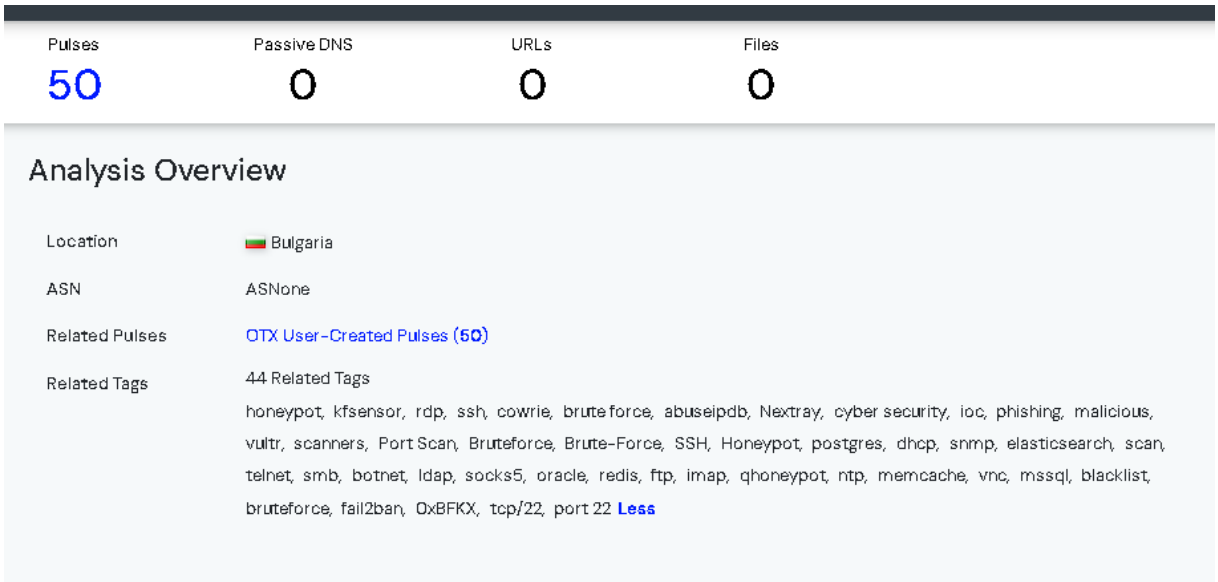
This IP address has been reported a total of **16,085** times from 1,316 distinct sources. 45.128.232.67 was first reported on May 27th 2023, and the most recent report was **6 months ago**.

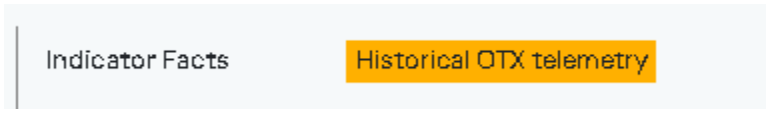
**Old Reports:** The most recent abuse report for this IP address is from **6 months ago**. It is possible that this IP is no longer involved in abusive activities.

| Reporter | IoA Timestamp (UTC) | Comment | Categories |
|---|---|---|---|
| ✔ Anonymous | 2025-07-24 00:06:09 (6 months ago) | $f2bV_matches | Brute-Force SSH |
| ✔ 🇩🇪 devsecops.cv | 2025-05-06 02:00:20 (9 months ago) | SSH brute-force detected | SSH |
| ✔ Anonymous | 2024-12-26 00:11:55 (1 year ago) | $f2bV_matches | Brute-Force SSH |
| ✔ 🇫🇮 quita.ch | 2024-07-26 02:13:08 (1 year ago) | 2024-07-26T04:12:25.361456+02:00 quita sshd[88695]: pam_unix(sshd:auth): authentication failure; log … show more | Brute-Force SSH |




2. ADIM: TERMİNOLOJİ VE YAPILANDIRMA

IOC (Indicator of Compromise) - Tehlikenin İzleri

IOC Nedir? IOC, bir siber saldırının gerçekleştiğine veya gerçekleşmek üzere olduğuna dair bıraktığı dijital izlerdir. Sadece IP adresi değil, zararlı dosyanın hash değeri, kötü domain adresi, saldırıda kullanılan URL veya zararlı yazılımın registry anahtarı da IOC olabilir.

Bu Vakadaki IOC Verisi:

IOC TİPİ: IPv4 Adresi

DEĞER: 45.128.232.67

NETWORK: 45.128.232.0/24

ASN: AS50053 (Anton Levin - NETERRA LTD.)

İLK TESPİT: 27 Mayıs 2023

SON AKTİVİTE: 6 ay önce (Temmuz 2025)

KAYNAK: SOC SIEM - Kritik Sunucu Log

İLİŞKİLİ DOMAIN: 67.232.128.45.pfdcloud.io

SSL SERTİFİKALARI: yahoo.com, vsk.si (Sahte sertifikalar!)

Diğer Potansiyel IOC'ler:

- İlişkili IP'ler: 45.128.232.238, 45.128.232.191
- Sahte SSL sertifikası hash'leri
- HTTP User-Agent: OmniSoftware

CTI (Cyber Threat Intelligence) - Veriyi İstihbarata Dönüştürmek

Sadece Veri (Data): "45.128.232.67 IP adresi Hollanda'da kayıtlı, NETERRA LTD firmasına ait."

İstihbarat (Intelligence) - Bağlam Ekleme: Bu IP adresi son 3 yılda 16,085 kez farklı kaynaklardan kötü amaçlı aktivite olarak raporlanmış. SSH brute-force saldırıları, port tarama ve honeypot sistemlerinde tespit edilmiş. AlienVault OTX platformunda 50 farklı tehdit kampanyasıyla ilişkilendirilmiş ve "botnet, phishing, malicious" etiketleri taşıyor.

Şirketimiz İçin Tehdit Neden Oluşturuyor? Kritik sunucumuz port 22 (SSH) ve port 445 (SMB) üzerinden bu IP ile iletişim kurmaya çalışmış. Bu portlar, dosya paylaşımı ve uzaktan erişim için kullanılır. IP'nin geçmişte SSH brute-force saldırıları yaptığı biliniyor, bu da sunucumuza şifre denemesi yaparak sızmaya çalıştığı anlamına geliyor. Eğer başarılı olursa, içerideki hassas verilere erişebilir veya sunucumuzu botnet ağına ekleyerek başka saldırılarda kullanabilir. Ayrıca bu IP sahte SSL sertifikaları kullanıyor, bu da man-in-the-middle (ortadaki adam) saldırısı yapmak için phishing sitesi olabileceğini gösteriyor.

MISP (Malware Information Sharing Platform) - Toplu Savunma

MISP Nedir? MISP, kurumların keşfettikleri tehdit bilgilerini (IOC'leri) birbirleriyle paylaştığı açık kaynaklı bir platformdur. Bir banka bu IP'den saldırı alırsa ve bunu MISP'e yüklerse, binlerce başka kurum otomatik olarak bu bilgiyi alır.

Diğer Kurumlar Nasıl Faydalanır?

1. Otomatik Engelleme: MISP ile entegre firewall'lar bu IP'yi otomatik olarak bloklar
2. SIEM Kuralları: Diğer SOC ekipleri bu hash değerini SIEM'de arar, bulaşma olup olmadığını kontrol eder
3. Email Gateway: Bu domain'den gelen mailleri otomatik karantinaya alır
4. Proaktif Tarama: EDR sistemleri bu dosya hash'ini tüm bilgisayarlarda tarar

Sonuç olarak, bir kurumun keşfi, binlerce kurumun savunmasını güçlendirir. Bu "toplu bağışıklık" prensibidir.

3. ADIM: KARAR VE AKSİYON

🔘 KARAR: ENGELLE

Konu: Kritik Sunucu - Şüpheli IP Bağlantısı

ÖZET:
Kritik sunucumuz SRV-FIN-01 ile 45.128.232.67 IP adresi arasında SSH (Port 22) üzerinden bağlantı denemesi tespit edildi. Yapılan istihbarat analizi sonucunda bu IP'nin yüksek riskli bir botnet kaynağı olduğu belirlenmiştir.

TEKNİK BULGULAR:

- Tehdit Geçmişi: Bu IP, 2023'ten bu yana 16,085 kez SSH brute-force, port tarama ve phishing aktiviteleriyle raporlanmış
- OTX Tehdit Skoru: 50 farklı siber tehdit kampanyasında aktif rol almış (botnet, honeypot tespiti, malicious scanners)
- Aktif Servisler: Bu IP üzerinde Apache/2.4.41 web sunucusu çalışıyor ve "OmniSoftware" başlıklı bir site barındırıyor (muhtemelen sahte yazılım indirme sitesi veya phishing sayfası)
- Sahte Sertifikalar: Yahoo.com ve vsk.si için sahte SSL sertifikaları barındırıyor (Man-in-the-Middle saldırısı ve phishing göstergesi)
- Son Aktivite: En son 6 ay önce (Temmuz 2025) SSH brute-force saldırısı gerçekleştirmiş
- Historical OTX Telemetry: Geçmişte AlienVault OTX platformunda kötü amaçlı aktivitelerle kaydedilmiş

RİSK DEĞERLENDİRMESİ:
Bu IP'nin sunucumuzla SSH üzerinden bağlantı kurması, otomatik şifre deneme saldırısı (brute-force) başlattığı anlamına geliyor. Eğer zayıf bir şifre varsa sisteme sızabilir, root erişimi elde edebilir ve ransomware yükleyebilir veya sunucumuzu kendi botnet ağına ekleyebilir. Ayrıca sahte SSL sertifikaları kullanması, phishing kampanyalarında aktif olduğunu gösteriyor.

ÖNERİLEN AKSİYONLAR:

1. Firewall Engelleme: 45.128.232.0/24 tüm subnet'i firewall'da acil olarak bloklanmalı
2. Sunucu Forensic: SRV-FIN-01 üzerinde zararlı yazılım taraması ve log analizi yapılmalı
3. SSH Log İnceleme: Başarılı login denemesi olup olmadığı kontrol edilmeli (/var/log/auth.log)
4. Şifre Değişimi: Sunucudaki tüm kullanıcı şifreleri güçlü parolalarla değiştirilmeli, 2FA aktif edilmeli
5. IOC Paylaşımı: Bu IP ve ilişkili IOC'ler MISP platformunda sektörle paylaşılmalı
6. Network Tarama: Diğer sunucularda da bu IP ile bağlantı olup olmadığı SIEM'de aranmalı

SONUÇ:
Bu IP adresinin brute-force geçmişi, botnet aktivitesi ve sahte sertifika kullanımı göz önüne alındığında acil müdahale gereklidir. Engelleme yapılmazsa veri ihlali veya ransomware bulaşma riski vardır.

# Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

1. RANSOMWARE SALDIRISI

İlk 3 Adım:

1. Ağdan İzole Et

- Ethernet kablosunu çek, Wi-Fi kapat
- Bilgisayarı kapatma, açık tut (RAM'deki veriler silinir, forensic analiz zorlaşır)
- Yan bilgisayarlara sıçramasını önle

2. Etkilenen Cihazları Tespit Et

- SIEM'de aynı zararlıyı ara
- File server'a bak, oralar şifreli mi?

3. Yedekten Kurtar

- Offline yedeklere bak
- Fidye ödeme son çare

Hangi Loglara Bakarım:

- Email Gateway: Phishing maili var mı?
- EDR Log: Hangi .exe çalıştı?
- Firewall: Zararlı IP'ye bağlantı var mı?
- Windows Event Log: Hangi process başladı?

2. PHİSHİNG MAİLİ

Sahteliği Kanıtlamak:

- Header'a bak: Return-Path gerçek göndereni gösterir
- SPF/DKIM: Fail ise sahte
- URL'yi kontrol et: Hover yap, garip domain var mı?
- IP'yi ara: AbuseIPDB'de daha önce raporlanmış mı?

Önlem:

Email Gateway:

Kural: Sahte domain'den gelen mailleri karantinaya al

Firewall:

Kural: Phishing URL'sini engelle

3. MAVİ TAKIM RUHU

Standart:

NIST SP 800-61

1. Hazırlık
2. Tespit
3. Sınırlama
4. Temizleme
5. Kurtarma
6. Ders Çıkarma

Kriz İletişimi -Ekip İçi:

- Sakin kal, görev dağıt
- 30 dakikada bir güncelle

4. GÜNCEL KALMA

The Hacker News

Linkedin 😊