ACFE TÜRKİYE ADLİ BİLİŞİM VE SİBER SUÇLARLA MÜCADELE ZİRVESİ

SUİSTİMAL VE BİLİŞİM RİSKLERİNİN YÖNETİLMESİ, VAKALARIN TESPİTİ, ANALİZİ VE DELİLLENDİRİLMESİNDE ADLİ BİLİŞİM METOTLARI VE TEKNOLOJİNİN ETKİN KULLANIMI

GÜNCEL RİSKLERE KARŞI ADLİ BİLİŞİM METOTLARI VE SİBER SUÇLARLA MÜCADELE YÖNTEMLERİ

- Adli Bilişim Nedir?
- Uzmanının sahip olması gereken vasıflar
- Delillerin incelenmesinde kullanılan araçlar
- Temel Adli Bilişim kavramları

-İşletim sistemleri ve karakteristik özellikleri
-Verinin sabit diskte nasıl saklandığı
-Tahsis edilmiş ve tahsis edilmemiş disk alanları
-Meta veri
-Dosya silme
-Şifreleme
-İşletim sistemi artifaktları
-Log dosyaları
-Windows kayıt defteri
Link dosyaları
Jump List
Prefetch dosyaları

DÜŞMANI TANIYALIM

- Ulus devletler
- Büyük organizasyonlar (özel istihbarat firmaları vb.)
- Organize guruplar (organize suçlular, aktivistler, teröristler vb.)
- Bireyler

DÜŞMANIN AMACI

- Endüstriyel casusluk
- Devlet casusluğu
- İçerden yapılan sızıntılar
- Şantaj
- Sabotaj
- Siber savaş
- Terörizm

SALDIRGANLARIN VE SUİSTİMAL İNCELEME UZMANLARININ KULLANDIĞI ARAÇLAR

Saldırganların Kullandığı Araçlar

1. Malware
    - Government Grade
    - Advanced Malware
2. Spyware
    - Government Grade
    - Commercial Grade
    - Hardware
3. Surreptitious Eavesdropping
4. Sosyal Mühendislik
5. Decryption Tools
6. Data Hiding
7. Forensic Hardware
8. Sniffers

SALDIRGANLARIN VE SUİSTİMAL İNCELEME UZMANLARININ KULLANDIĞI ARAÇLAR

Suistimal ve İnceleme Uzmanlarının Faydalanabileceği Araçlar

1. Adli Bilişim Araçları
    - FTK
    - Encase
    - Forensic Explorer
    - X-Ways
    - Axiom
    - Blackbag
    - Enterprise Level Tools
    - Bellek Analizi
2. Mobil Adli Bilişim Araçları
    - Cellebrite
    - Oxygen
    - Paraben
3. Adli Bilişim Donanımları
    - Tableau
    - CRU
    - Others

SORUŞTURMA VE İNCELEMEDE GÜNCEL YÖNTEMLER VE - VAKA ANALİZLERİ

Olay Yönetimi

1.İlk Müdahale

a) Dijital suç mahali

b) Delil toplama yöntemleri

c) Dijital delillerin işlenmesi

d) Dijital delillerin incelenmesi

2. Kontrol altına alma

a) Saldırganın tanımlanması

b) Saldırganın erişiminin duraklatılması

c) Saldırganın erişiminin tamamen durdurulması

3. Hasarın onarılması

a) Ne, nasıl, ne zaman ve kim tarafından yapıldı tespit etmek için detaylı inceleme

b) Temizlik ve onarım

VAKA ÖRNEKLERİ

1. Cep telefonuna kurulan gelişmiş spyware vakası
2. Fortune 100 listesindeki bir şirket, şirket ağında Gelişmiş Dosyasız Zararlı Yazılım tespit edilmesi
3. Phishing Saldırısı
4. İş e-postasının ele geçirilmesi vakaları
5. Hukuk bürosunun şirket ağına sızılması vakası

BİLGİ GÜVENLİĞİ VE ENDÜSTRİYEL CASUSLUĞA KARŞI KOYMA TEKNİKLERİ

BT Güvenliği: Önleme Ve Tespit Etme

1. Anti-Virüs
2. Güvenlik Duvarları (Firewalls)
3. Yetkisiz Erişim Engelleme Sistemleri (Intrusion Prevention Systems)
4. Yetkisiz Erişim Tespit Sistemleri (Intrusion Detection Systems)
5. Ağ Adli Bilişimi (Network Forensics)
6. Sistem Sıkılaştırma (Computer Hardening)
7. Hava Boşlukları (Air Gaps)

BİLGİ GÜVENLİĞİ VE ENDÜSTRİYEL CASUSLUĞA KARŞI KOYMA TEKNİKLERİ

ENDÜSTRİYEL CASUSLUĞA KARŞI KOYMA TEKNİKLERİ

- Saldırganların kullandığı araçlar ve teknikler

- Bilgi güvenliği, soruşturma ve inceleme uzmanları tarafından bunları tespit etmede kullanılan araçlar ve teknikler

CONTACT INFO

CyberDiligence.com

yd@Cyberdiligence.com