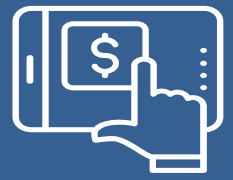
ISO 9001 2015 CERTIFIED



BİLGİKORU
SİBER GÜVENLİK

BİLGİKORU
Digital Technology

Sızma Testi Nedir ?

www.bilgikoru.com

100. Yıl Bulvarı No:55/E/21
Ostim Teknopark Ankara

GÜNDEM

- BİLGİKORU kimdir?
- Sızma Testi nedir?
- Sızma Testi Neden Yapılır?
- Sızma Testi Metodolojileri (White/Black/Grey)
- Sızma testi türleri nelerdir? (Web, Network, Mobil, vs…)
- Bir sızma testi uygulaması yapılırken uygulanan süreçler nelerdir?

BİLGİKORU KİMDİR?

Siber güvenlik

Sızma Testleri

Yönetilen Güvenlik

Sistem Kurulumu

SOME

Adli Bilişim

Uzman Mütalaası

Bilirkişi Hizmetleri

Siber Suç İnceleme

Veri Kurtarma

Fiziksel Hasar Görmüş Materyaller

Şifrelenmiş Veriler

KVKK ve Güvenlik Süreçleri

KVKK

ISO 27001

Vizyonumuz, Türkiye'de ve dünyada bilişim güvenliği denince; çözüm sağlayıcı, katma değerli hizmetler üreten, etkin ve güvenilir olarak akla gelen ilk isimlerden biri olmaktır.

SIZMA TESTİ NEDİR?

- **Sızma testi**, sistemin güvenliğini değerlendirmek üzere bir bilgisayar sistemi üzerinde gerçekleştirilen yetkilendirilmiş temsili bir siber saldırıdır.

- **Sızma testinde** beklenen, dışarından bir gözle sistemsel ve yazılımsal açıklıkların bir uzman tarafından tespit edilerek raporlanmasıdır.

- **Sızma testi** raporu doğrultusunca şirketler, sistemleri ile ilgili zafiyetleri öğrenerek bunları kapatma veya güvenliğini arttırma yoluna gitmektedirler.

SIZMA TESTİ NEDEN YAPILIR

- Sızma Testi Kanunu bir zorunluluktur
  - BDDK(BSD.2012/1)

  Güvenlik ile ilgili hükümlerin gereklerinin yerine getirilmesi hususunda herhangi bir icrai görevi bulunmayan bağımsız ekiplere düzenli aralıklarla sızma testleri yaptırılır.
  - EPDK(30123 sayılı Resmi Gazete)

  Doğrudan pentest (sızma testi) yükümlülüğü getirmese de ISO27001 zorunluluğu getiren EPDK lisans yönetmelikleri dolayısıyla enerji sektöründe de sızma testi ihtiyacı ortaya çıkmıştır.
  - SPK(VII-128.9)

  Bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal ve uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az bir yılda bir kez sızma testine tabi tutulur.
- Sızma Testi Bilgi Güvenlik Süreçlerinin en önemli parçalarından birisidir
  - ISO 27001
  - PCI-DSS
  - COBIT
  - ITIL

SIZMA TESTİ NEDEN YAPILIR

- **Saldırganın / Hacker'ın motivasyonu nedir?**
  - Kişisel fayda sağlamak
  - Muhatabına maddi zarar vermek
  - Bir işin başarılabildiğinin göstermek
  - Kurum/ kuruluşun küçük düşürülmesi
  - kişisel intikam hissi

- **Test Yaptırmanın amacı nedir?**
  - Temelde siber zafiyetlerin görülmesi,
  - Açıkların tespit edilerek saldırganların giriş noktalarının tespit edilmesi,
  - Felaket durumlarında hızlı aksiyon alma ihtiyacı

SIZMA TESTİ NEDEN YAPILIR

- **Sızma Testi yaptırarak,**
  - Bilinen zafiyetlerden kurum/ kuruluşun ne seviyede etkilendiği,
  - Saldırı anında hangi sistemlere daha çok önem verilmesi gerektiği,
  - Meydana gelecek kaybın tahmin boyutları tespit edilir.

SIZMA TESTİ METODOLOJİLERİ NELERDİR

- **WHITE BOX**
  - Kurum içerisinden çok miktarda bilgi verilerek yapılan testlerdir.
  - Yüksek seviye bir yönetici veya admin seviyesi kullanıcı hesabının hacklenmesi ile olabilecek durumlar test edilir.

- **GRAY BOX**
  - Bu türde test uzmanına standart bilgiler verilerek, normal bir personel hesabı hackleyen saldırganın yapabilecekleri görülür.

- **BLACK BOX**
  - Siber uzmana hiçbir bilgi verilmez. Tamamen dışarda bir saldırgan gözü ile saldırılar yapılır.

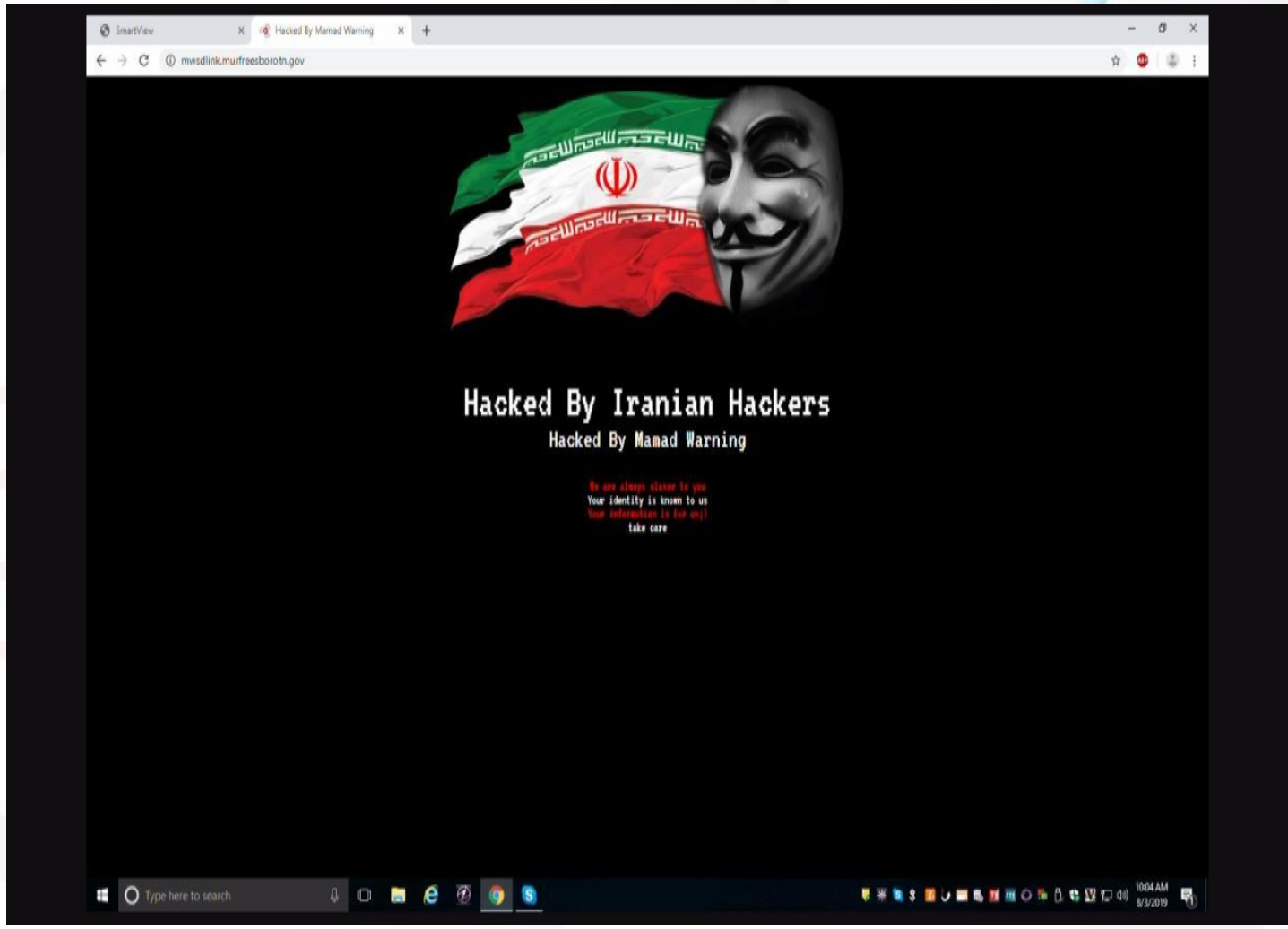
Sızma Testi Türleri

- WEB Sızma Testi
- Local Network Sızma Testi (LAN)
- Mobil Uygulama Sızma Testi
- Kablosuz Ağ Sızma Testi (Wireless)
- Sosyal Mühendislik Testleri
- Hizmet Durdurma (DOS/ DDOS) Testleri
- Dahili Telefon hatları (VOIP) Sızma Testleri
- USB Zafiyet Testleri

SIZMA TESTİ TÜRLERİ - WEB PENTEST

➢ WEB Sızma Testi

- Girdi alanlarının kontrolü,
- XSS payload denemeleri,
- SQL Injection kontrolleri,
- Default bırakılmış dosya, parola vb.
- File inclusion & File Upload açıkları
- Server-Side Exploitation
- Admin paneline erişim



SIZMA TESTİ TÜRLERİ - Wireless Sızma Testi

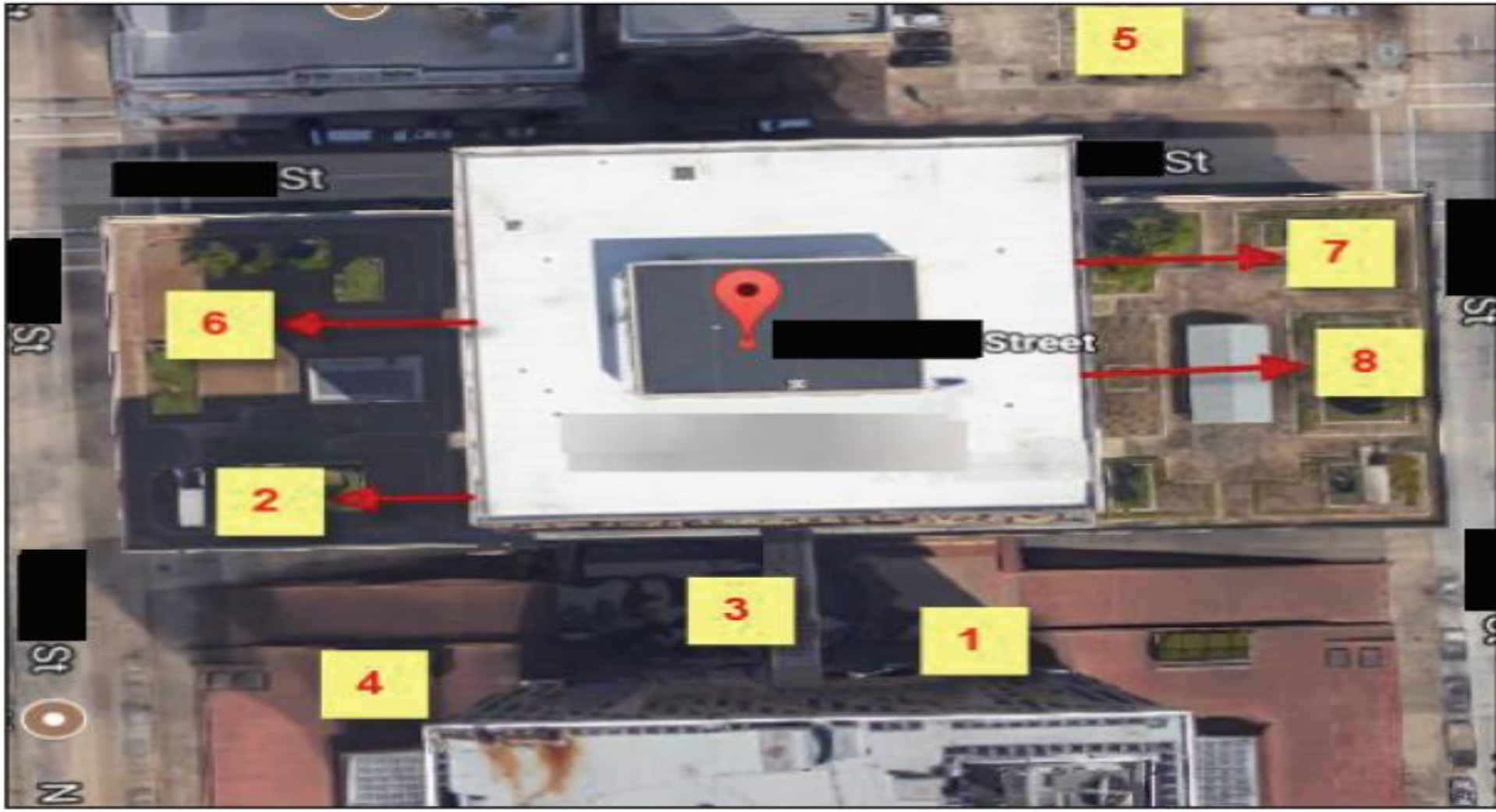
- Wireless Sızma Testi

1) AP tarama testleri
2) AP şifreleme türünün belirlenmesi
3) AP Deauth testlerinin yapılması
4) MAC koruma olup-olmadığının varsa atlatılabilme testlerinin yapılması
5) WEP şifreleme için IV toplama ve ağa dahil olma testleri
6) WEP şifreleme için ağda bağlı kullanıcı olmaması durumda parolanın ele geçirilerek ağa bağlanma testleri
7) WPA/ WPA2 şifrelemelerde Brute-Force testleri
8) WPA/ WPA2 testlerde veritabanı kullanarak parolanın ele geçirilmesi işlemleri
9) Erişim noktasının farklı noktalarda sinyal seviye testleri
10) WPS zafiyeti testleri
11) WPS PIN numarasının ele geçirilme testleri
12) Gizli Wireless ağların menzile girenlerinin tespit edilmesi, sinyal seviyelerinin raporlanması
13) Kablosuz ağ haritasının çıkartılması
14) Kablosuz ağ menzilinde bulunan tüm diğer ağların bulunarak raporlanması

SIZMA TESTİ TÜRLERİ - Wireless Sızma Testi

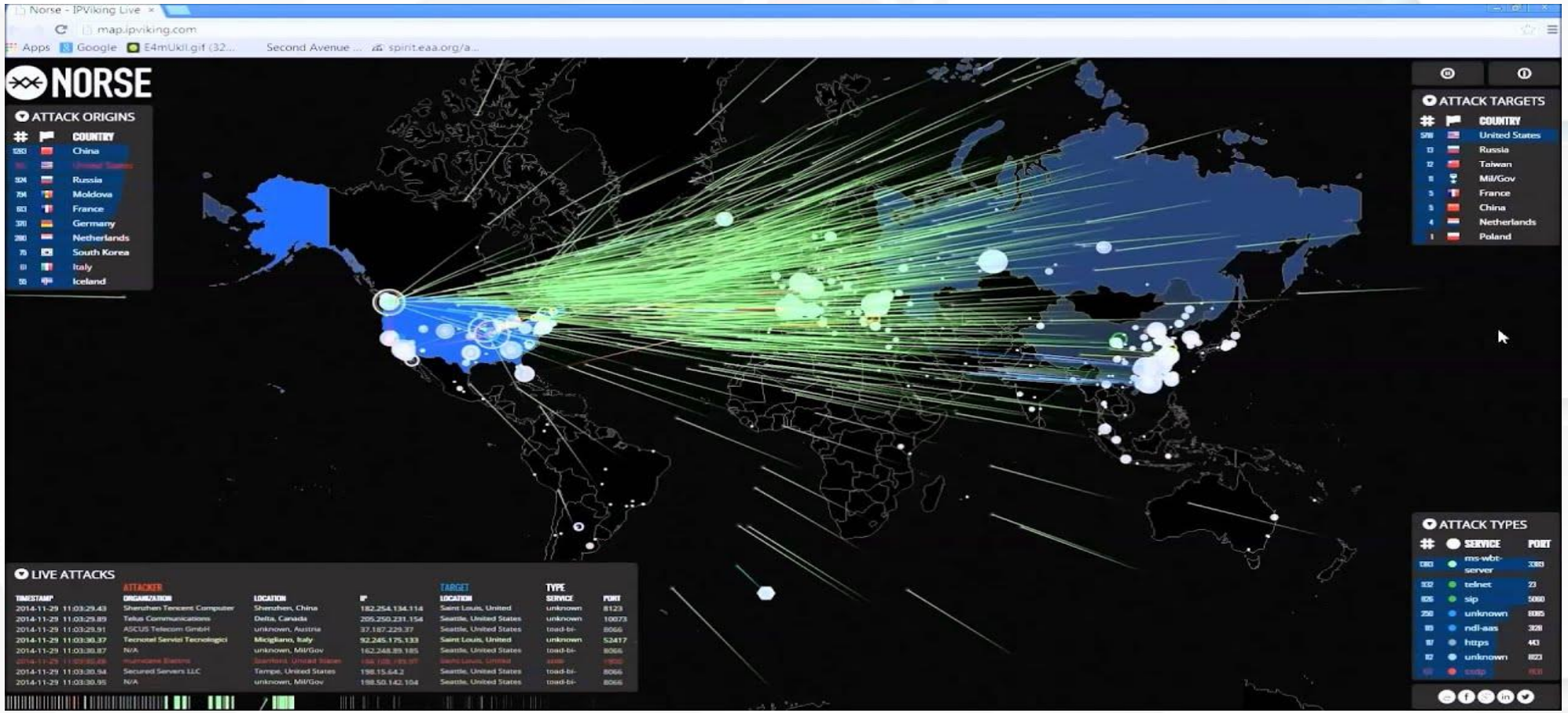
- Wireless Sızma Testi
  (Signal MAPPING)

Figure 11: Map of Signal Testing Locations

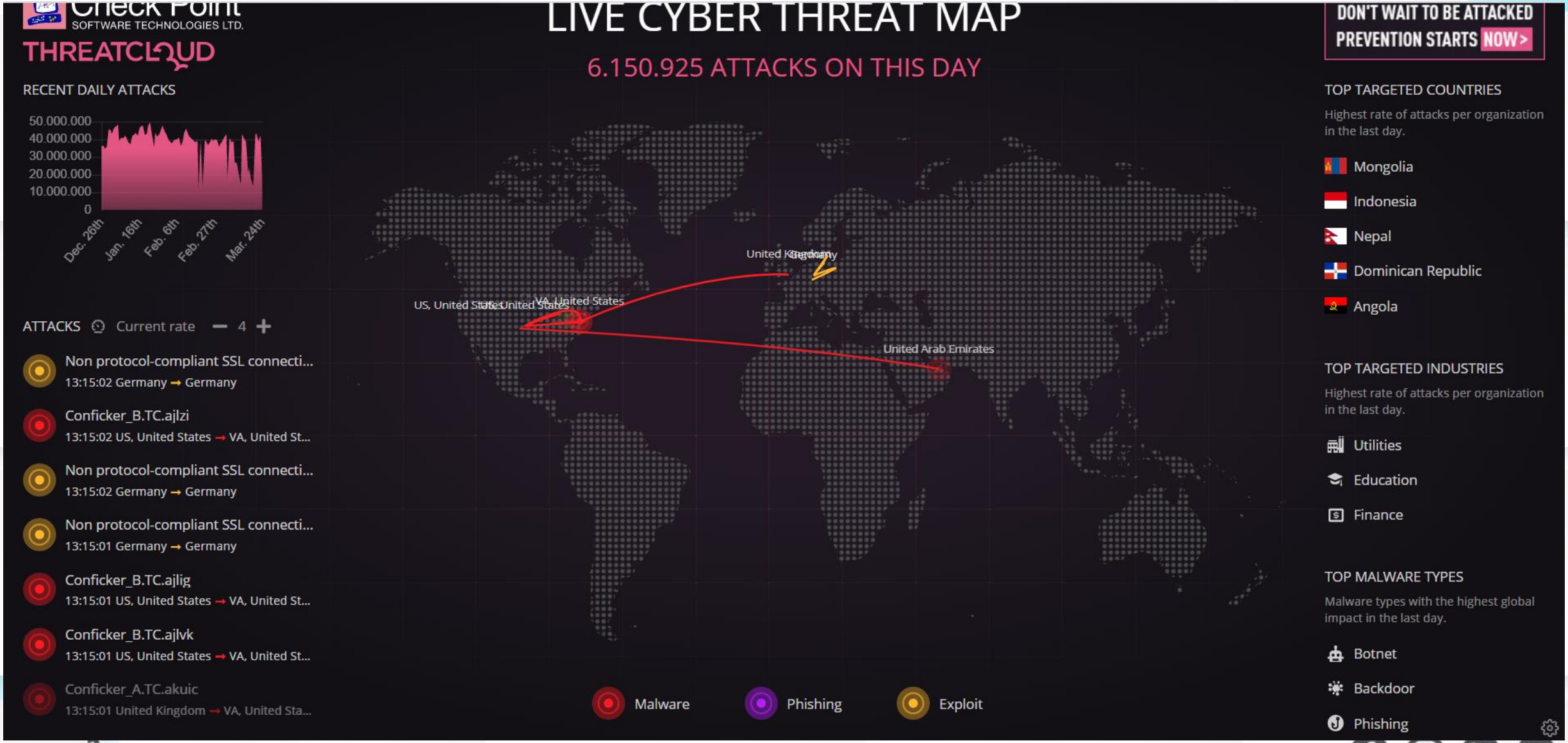


SIZMA TESTİ TÜRLERİ - DOS – Hizmet Durdurma

- Sistemin kabul edemeyeceği miktarda yükün, sisteme gönderilmesi ile yapılan, hizmeti durdurmaya yönelik saldırı türüdür.



SIZMA TESTİ TÜRLERİ - Live Attack MAP



SIZMA TESTİ TÜRLERİ - LAN Sızma Testi

- Local Area Network (LAN) Sızma Testi

SIZMA TESTİ TÜRLERİ - LAN Sızma Testi

- Local Area Network (LAN) Sızma Testi
  - Amaç, saldırgan kişinin sizin sistem odanıza girememesidir.
  - Phishing, yanlış yapılandırma, sistemsel veya yazılımsal zafiyetlerden ötürü sistem odanıza giren bir saldırgan, sunucularınızda bulunan her bilgiyi ele geçirebilir.
  - Buradaki asıl hedef, tehtidin sadece dışardan değil içerden de olabileceğini göstermektir.
  - İşten çıkarılan bir personel veya şirkete zarar vermek isteyen bir şahşın, ne kadarlık bir zarar vereeğin simüle edilerek raporlanır.
  - Çeşitli exploitlerin denenmesi, MITM saldırıları, ARP poison, MAC flood atakları, vlanlar arası erişimin sağlanma çalışmaları, sunucu zafiyetleri, dahili network taramaları, linux sunucular içerden erişim/ bağlanma testleri, bu sızma testi türünü temelini oluşturmaktadır.

SIZMA TESTİ TÜRLERİ – MOBİL & SOSYAL MÜHENDİSLİK

- Mobil Uygulama Sızma Testi,
  - Şirketin kurumsal mobil uygulaması üzerinde, kod analizi, SSL Pinning, web servis tespiti gibi analizler yapılarak bulunan zafiyetler raporlanır.
  - Ortak veritabanın kullanımında sadece web uygulamasının güvenli tutmak, mutlak güvenlik için yeterli olmayacaktır.

- Sosyal Mühendislik Testleri,
  - Kurumların isimlerine ve faaliyet gösterdiği alanlara yönelik sosyal mühendislik scriptleri (küçük yazılım parçaları) hazırlanarak testler yapılır.
  - Yetkili personel dışında kuruma bilgi verilmez ve olabilidiğince doğal sonuçlar alınmaya çalışılır.

SIZMA TESTİ TÜRLERİ – VOIP & USB

- Dahili Telefon hatları (VOIP) Sızma Testleri,
  - Dışardan shell alan veya içerden saldıran bir saldırganın VOIP santral üzerinden sisteme sızması, yapılan dahili telefon görüşmelerinin dinleyip- dinleyemediğinin tespiti yapılır.
  - Kurum içi yapılan görüşmelerin, kurum dışına çıkmaması için gerekli güvenlik önlemleri alınır.

- USB Zafiyet Testleri,
  - STUXNET benzeri durumlar ile karşılaşılmaması için fiziksel port güvenlik önem arz etmektedir.
  - Bu bağlamda özellikle kritik sunucu ve domain admin kullanıcı grubunda bulunan, yüksek erişebilirliğe sahip kullanıların bilgisayarlarında USB port sızma testleri yapılarak, zafiyetlerin ne boyutta olduğu görülür.
  - USB portların durum ile ilgili bir güvenlik prosedürü uygulanır.

SÜREÇLER - NE YAPILMALI?

- Unutulmamalıdır ki SIZMA TESTİ bir SALDIRI SİMÜLASYONUdur.
- Siber saldırı altında yaşayacağız kayıplar bu testler altında ortaya çıkmaktadır.
- Dünya üzerinde günde 6 milyondan fazla siber saldırı olmaktadır. (Malware, Phishing, DDOS, web hacking vs.)
- "Türkiyede ise sadece 2019 yılının ilk çeyreğinde, toplam 1.2 milyondan fazla, günde ise ortalama 13 bin 842 adet oltalama saldırısı gerçekleşmiştir." (Kaynak: *https://www.haberturk.com/siber-saldirilar-2019-yilinda-hangi-ulkeleri-hedefliyor-2446393-teknoloji*)

- **Adli Bilişim** Eğitimi
-
- **Veri Kurtarma** Eğitimi
- **Siber Güvenlik** Eğitimleri
  - Temel Seviye
  - İleri Seviye

- **LINUX** İşletim Sistemi Eğitimi
- **PYTHON** Yazılım Eğitimleri
  - Temel Seviye
  - İleri Seviye
- **Kurum içi Bilgi Güvenliği Farkındalık** Eğitimi

www.bilgikoru.com

BİLGİKORU
Digital Technology

TEŞEKKÜRLER

100. Yıl Bulvarı No:55/E/21 Ostim Teknopark ANKARA
E-mail: bilgi@bilgikoru.com **Tel:** 0 (312) 354 77 33

ISO 9001 2015 CERTIFIED