
CATCH PROBE™
INTELLIGENCE TECHNOLOGIES
SMARTDECEPTIVE
OTD BİLİŞİM
GLOBAL VAD

SMARTDECEPTIVE: SALDIRGANLARI GÖRÜNMEZ KILMAK

SMARTDECEPTIVE NASIL İŞLER?

SmartDeceptive teknolojisi, meşru ağ varlıklarını, hizmetlerini veya verilerini taklit etmek amacıyla tasarlanmış aldatma sistemlerinin ve tuzaklarının devreye alınmasını ifade eder. Bu aldatmalar, saldırganları çekmek, onları gerçek sistemlerden uzaklaştırmak ve davranışları hakkında istihbarat toplamak için stratejik bir şekilde konumlandırılır. SmartDeceptive çözümleri, gerçek ağı tehlikeye atmadan saldırganlarla aktif bir şekilde etkileşimde bulunur ve IP adresleri, saldırı yöntemleri, araçlar ve etki alanı adları gibi kritik verileri ele geçirir.

SMARTDECEPTIVE NASIL İŞLER?

• SmartDeceptive Yemler (Decoy'lar) ve Tuzaklar: Bu aldatıcılar, cihazlar, sunucular, uç noktalar veya uygulamalar biçiminde ortaya çıkabilir. Gerçekten de varmış gibi görünseler de, saldırganları yanıltmak amacıyla tasarlanmışlardır.

• Saldırgan Etkileşimi: Bir saldırgan yemle etkileşime geçtiğinde, sistem onların taktikleri, teknikleri ve prosedürleri (TTPs) hakkında değerli bilgiler toplar.

• Gerçek Zamanlı İzleme ve Uyarılar: Güvenlik ekipleri, sahte hedefler devreye girdiğinde anında uyarılar alır ve bu durum, tehditleri gerçek zamanlı olarak analiz etme imkanı sunar.

• Veri Toplama ve Analizi: Sistem, IP adresleri ve saldırı vektörleri gibi ayrıntıları yakalayıp kaydeder. ve kullanılan araçlar, kuruluşların düşman davranışlarını analiz ederek savunmalarını güçlendirmelerine

SMARTDECEPTIVE AVANTAJLARI

• Proaktif Savunma:
SmartDeceptive, organizasyonların saldırganları saldırı yaşam döngüsünün başlangıç aşamalarında gerçek varlıklara zarar vermeden önce tespit eder .

• Doğru Tehdit İstihbaratı:
Saldırganlarla doğrudan etkileşimde bulunarak, aldatma teknoloji, tehdit istihbaratını ve müdahale çabalarını güçlendiren son derece özel veriler sunar.

• Düşük Yanlış Pozitif Oranı:
Sahte hedefler, normal ağ trafiği için tasarlanmadığından, bunlarla gerçekleştirilen etkileşimlerin büyük olasılıkla kötü niyetli olması, yanlış pozitifleri en aza indirir.

• Artan Olay Müdahale Verimliliği:
SmartDeceptive, olay müdahale platformlarıyla entegre çalışarak, güvenlik ekiplerine doğrulanmış tehditleri artırır.

NERELERDE UYGULANABİLİR?

• Dahili Ağlar:
Veritabanları gibi hayati iç varlıkları koruyun ve çalışanların kimlik bilgilerini sahte hedefler aracılığıyla ele geçirin.

• Bulut Ortamları:
Bulut tabanlı uygulamaları, konteynerleri ve sanal makineleri taklit eden yemler oluşturarak bulut altyapılarını güvence altına alın.

• IoT Sistemleri:
Kameralar, yazıcılar veya endüstriyel kontrol sistemleri (EKS) gibi bağlı cihazları simüle eden tuzaklar dağıtarak IoT ağlarını güvence altına alın.

• Operasyonel Teknoloji (OT):
Endüstriyel ortamlara özgü aldatma tekniklerini kullanarak OT sistemlerini ve kritik altyapıyı (SCADA sistemleri gibi) koruyun.

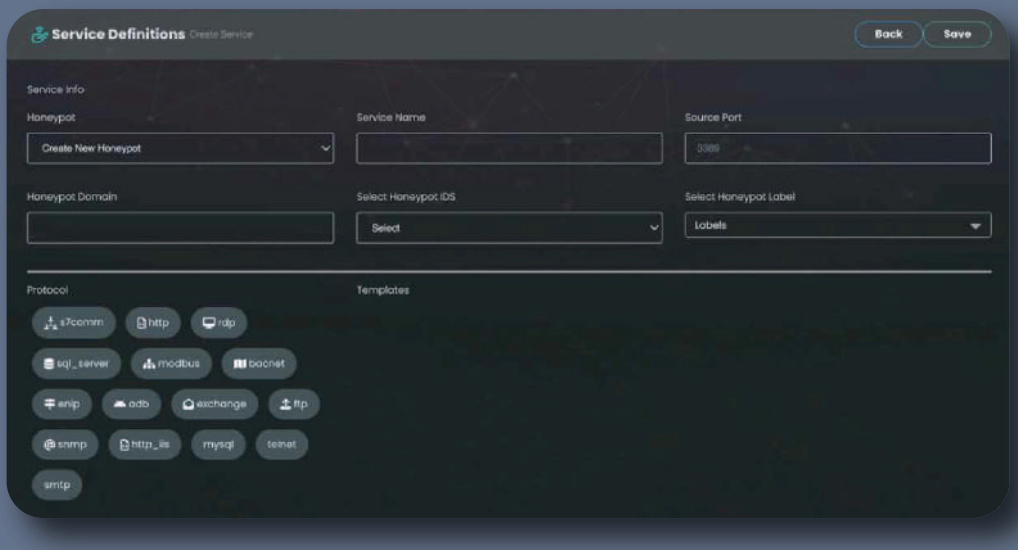
SMARTDECEPTIVE: Gerçek Zamanlı Tehdit İstihbaratı için Aldatma Teknolojisi

CatchProbe SmartDECEPTIVE, aldatmaca tuzaklarını dağıtmak ve yönetmek, ayrıntılı siber istihbarat toplamak ve saldırgan faaliyetleri gerçek zamanlı olarak izlemek amacıyla tasarlanmış kapsamlı bir aldatma yönetim platformudur. Kuruluşları korumak için eyleme geçirilebilir içgörüler sunmak üzere ThreatWAY ve LeakMAP ile sorunsuz bir entegrasyon sağlar.

Temel Ayırt Edici Özellikler

Hızlı Kurulum

Dakikalar içinde konuşlandırılabilen sahte hedefler, karmaşık kurulumlar veya kapsamlı yapılandırmalar gerektirmeden hızlı bir savunma sunar.



Platformlar Arası Kurulum

SmartDECEPTIVE, geniş bir protokol ve hizmet yelpazesini desteklemektedir.

DECOY İŞLETİM SİSTEMİ TİPLERİ

Windows	Linux	Android	IoTs, Printers, Ca

UYGULAMALAR | İHTİYAÇLARINIZA GÖRE ÖZELLEŞTİRİLEBİLİR.

Microsoft

- Microsoft Exchange Server
- Microsoft IIS Server
- Microsoft SQL Server
- Microsoft RDP Server
- Microsoft Dynamics AX
- Microsoft Dynamics NAV
- Microsoft Sharepoint

Linux

- HTTP
- SMTP
- FTP
- TELNET-DNS
- SSH
- SMB
- PhpMyAdmin

ICS/SCADA

- Modbus
- S7comm
- ENIP
- BACnet

- Mobile & Android
- Elasticsearch
- SAP
- FORTINET
- CHECKPOINT
- SOLARWINDS
- PASTEBIN
- On-Demand

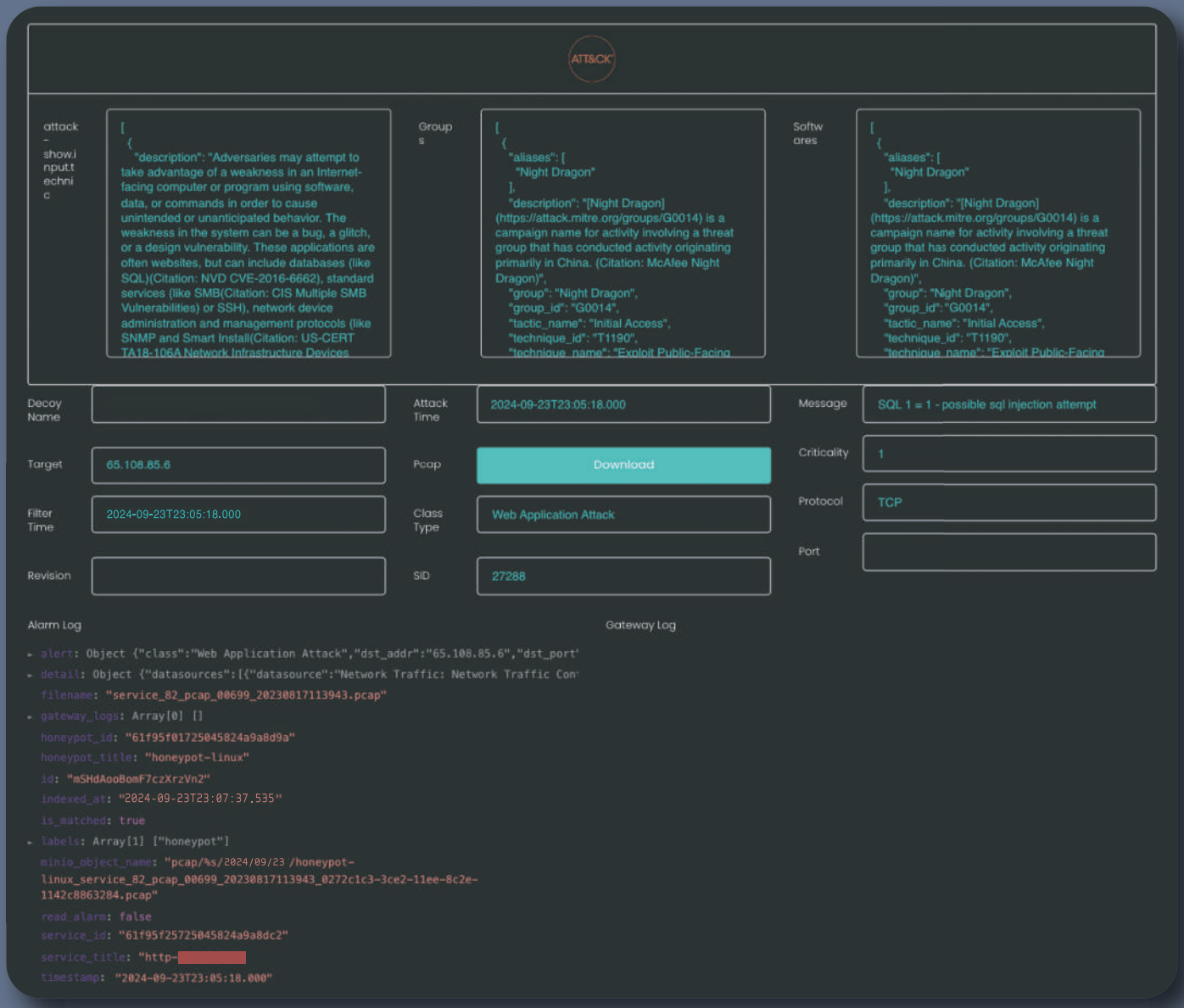
OTD BİLİŞİM
GLOBAL VAD

Maliyet Verimliliği

Ek bir lisanslama veya donanım maliyeti bulunmamaktadır; yemler, bu ortamları simüle etmek amacıyla veritabanı veya uygulama lisansları gibi ek satın alımlar gerektirmez.

Derinlemesine İnceleme

Tam paket yakalama (PCAP) yeteneği ve Mitre Att&ck entegrasyonu ile Smart DECEPTIVE, saldırgan davranışının kapsamlı bir şekilde anlaşılmasını sağlayan detaylı bir analiz sunar.

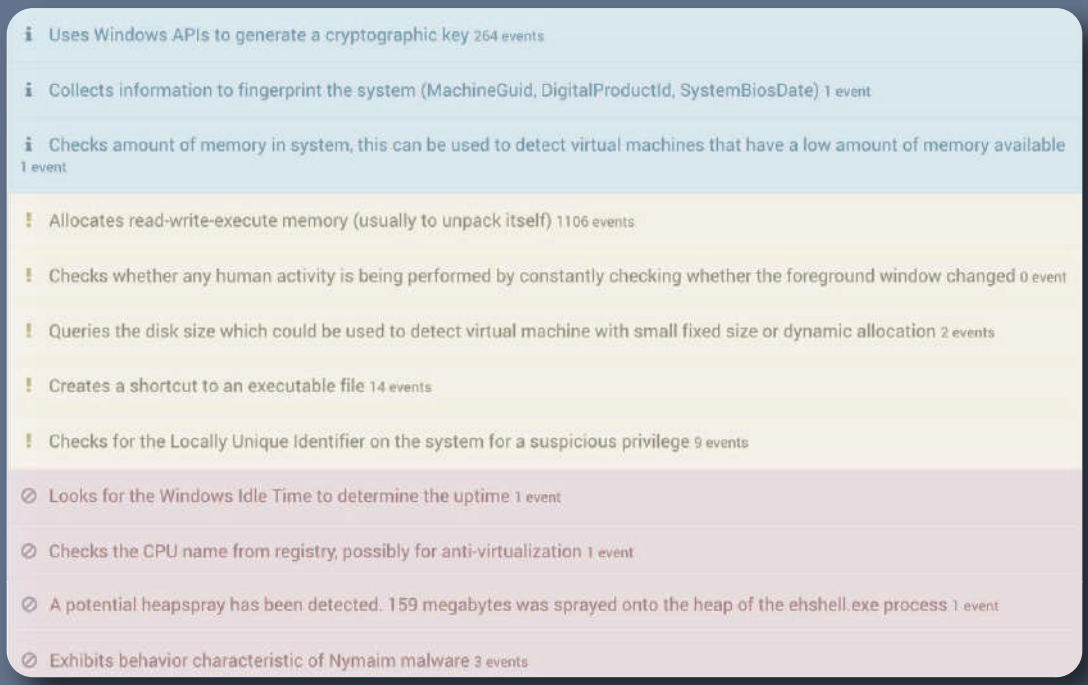


Yapay Zeka ile Hazırlanan Raporlar ve Öneriler

SmartDECEPTIVE, tespit edilen tüm saldırıları analiz eden, savunmaları güçlendirmek ve gelecekteki riskleri azaltmak amacıyla eyleme dönüştürülebilir önerilerle birlikte kapsamlı içgörüler sunan yapay zeka destekli raporlar sağlar.

Kötü Amaçlı Yazılım İncelemesi

Saldırganlar bu tuzaklara kötü niyetli yazılım yükleyerek, müşterilerin kötü niyetli yazılım hakkında kapsamlı analizler almasına olanak tanıyabilir.



Diğer Önemli Nitelikler

- Gerçek Zamanlı Durum İzleme
- Uzun Süre Fark Edilmeden Çalışma
- Zengin ve Özelleştirilmiş Senaryolar
- Hızlı Kurulum
- Tam PCAP Yetenek Özelliği
- Veri Zenginleştirme ve TTP Analizi
- EKS Senaryoları
- Tehdit Profillemesi ve İtibar Derecelendirmesi
- Uyarı ve Raporlama Becerileri
- SandBox'ta Otomatik Kötü Amaçlı Yazılım İncelemesi
- Exploit, Kötü Amaçlı Yazılım ve Shellcode Tespiti

Esnek Dağıtım Sistemi

SmartDECEPTIVE tuzakları, şirket içinde veya bulut ortamında konuşlandırılabilir.

ThreatWAY LeakMAP ile Entegrasyon

SmartDECEPTIVE, otomatik olay müdahalesi için ThreatWAY ile entegre olur ve hedefli saldırıları tespit etmek ile sızdırılan verilerin kötü niyetli amaçlarla kullanılma girişimlerini belirlemek için LeakMAP ile iş birliği yapar.

SmartDECEPTIVE

CATCHPROBE™

Decoy Sistemi Nedir?

Bir aldatmaca sistemi, savunmasız sistemleri veya ağları simüle ederek potansiyel saldırganları çekmek ve tuzağa düşürmek amacıyla tasarlanmış bir siber güvenlik mekanizmasıdır. Temel hedefi, saldırganların faaliyetleri hakkında değerli içgörüler sunarak, saldırı girişimlerini tespit etmek, saptırmak veya incelemektir. Aldatma sistemleri, siber suçlulara meşru hedefler gibi görünerek onları aldatmaya teşvik ederken, güvenlik uzmanlarının eylemlerini izlemelerine ve kritik verileri toplamalarına olanak tanır.

Sistem Nasıl İşler?

Bir aldatma sistemi, saldırganları çekmek ve davranışlarını analiz etmek amacıyla savunmasız bir sistemi, ağı veya uygulama ortamını simüle ederek faaliyet gösterir. Sahte hedef, bir sunucu, uygulama, veritabanı veya ağ hizmeti gibi meşru bir hedefe benzer şekilde yapılandırılır. Kullanıcı hesapları, dosyalar veya ağ trafiği gibi gerçekçi ancak sahte verilerle doldurularak, gerçek bir sistem izlenimi yaratılır. Ağ paketleri, oturum açma girişimleri ve diğer etkileşimler dahil olmak üzere gelen ve giden tüm trafiği yakalamak için izleme araçları sahte hedefe entegre edilmiştir.

Bir saldırganın sahte hedef içinde gerçekleştirdiği her eylem, yürütülen komutlar, erişilen veya değiştirilen dosyalar ve bırakılan tüm kötü amaçlı yazılımlar dahil olmak üzere titizlikle kaydedilir. Saldırgan sahte hedefle etkileşime girdiğinde, sistem yöntemlerini ve tekniklerini kaydeder. Düşük etkileşimli sahte hedefler yalnızca temel yanıtları simüle edebilirken, yüksek etkileşimli sahte hedefler daha gerçekçi bir ortam sunar. Aldatma sisteminde tespit edilen şüpheli aktivite hakkında güvenlik personelini bilgilendirmek için gerçek zamanlı uyarılar ayarlanabilir. Toplanan istihbarat, yeni güvenlik açıklarını, kötü amaçlı yazılımları ve saldırı vektörlerini belirlemeye yardımcı olarak genel tehdit istihbaratına katkıda bulunur.

Aldatma Teknolojilerinin Kullanımının Avantajları

Bir kurumsal ağda aldatma teknolojilerini kullanmanın birçok avantajı bulunmaktadır:

Erken Tehdit Algılama: Aldatma sistemleri, kötü niyetli faaliyetleri kritik sistemlere ulaşmadan önce tespit edebilir; geleneksel güvenlik önlemlerini aşabilen sıfırıncı gün istismarları da dahil olmak üzere yeni ve ortaya çıkan tehditleri belirleyebilir.

Tehdit Analizi: Aldatma tuzakları, saldırganların taktikleri, teknikleri ve prosedürleri (TTP'ler) hakkında ayrıntılı bilgiler sunar. Bu davranışları anlamak, kuruluşların daha sağlam savunma stratejileri geliştirmesine ve genel tehdit istihbaratını artırmasına yardımcı olur.

Dikkat Dağıtma ve Aldatma: Tuzaklar, saldırganların dikkatini dağıtarak zamanlarını ve kaynaklarını boşa harcayabilir ve onları gerçek hedeflerden uzaklaştırabilir. Bu sistemler ayrıca kötü niyetli içeridekileri aldatma unsurlarıyla etkileşime girmeye teşvik ederek tespit edebilir.

Verimli Kaynak Tahsisi: Aldatma teknolojileri, güvenlik kaynaklarının daha odaklı bir şekilde tahsis edilmesini sağlayarak çabaları gerçek tehditlere yoğunlaştırır ve geniş, genelleştirilmiş savunmalara olan ihtiyacı azaltır.

Decoy Çeşitleri:

Saldırı kalıplarını, kötü amaçlı yazılım davranışlarını ve yeni istismarları analiz etmek amacıyla kullanılır. Bu tuzaklar toplar.doğrudan savunma yerine araştırma amacıyla istihbarat.
Örnek: Botnet faaliyetlerini izlemek için oluşturulan bir tuzak ağı.
Üretim Tuzakları: Saldırıları erken tespit ederek güvenliği artırmak amacıyla devreye alınır. Gerçek tehditler için bir uyarı sistemi işlevi görürler.
Örnek: Kimlik avı girişimlerini tespit etmek için kurulan bir e-posta sunucusu tuzağı.

SmartDECEPTIVE

CATCHPROBE™

HERHANGİ BİR RİSK MEVCUT MU?

Perspektif	Geleneksel Honeypot'lar	SmartDECEPTIVE Decoys
Saldırganlar Tarafından Belirlenme	Uzman saldırganlar tarafından tespit edilebilirler.	Son derece etkileşimli, tespit edilmesi neredeyse imkansız.
Saldırıların Artışı	İzole edilmediği takdirde tırmanma riski bulunmaktadır.	Gerçek sistemle etkileşim bulunmamaktadır, tırmanma riski mevcut değildir.
Kaynak İhtiyacı	Önemli kaynaklar talep eder.	Bulutta konuşlandırılmıştır, kaynak gereksinimi yok
Yanlış Pozitifler	Yanlış pozitif, yorgunluğa neden olur.	Yapay zeka ile desteklenen saldırı analizi
Performans Problemleri	Ağ performansını etkileyebilir.	Bulutta konuşlandırılmıştır, ağ performansına etkisi yok
Yanlış Yapılandırma	Yeni güvenlik açıklarının ortaya çıkma olasılığı	Yanlış yapılandırma riski bulunmamaktadır.
Aşırı Bağımlılık Durumu	Sahte hedeflere aşırı güven duyulmasına neden olabilir.	Dayanıklılık amacıyla dört modül içeren bir platformun bileşeni.

SmartDECEPTIVE

CATCHPROBE™

HACKER'IN PERSPEKTİFİNİ ANLAMAK

İlk Keşif: Sana yolumu nasıl bulduğumu göstereyim.

OSINT, SIGINT, HUMINT – hepsi klasiklerdir.

Google? O senin en yakın dostun... ve benim de.
Forumlar mı? Altın madenleridir. Resmi Cisco veya Oracle forumlarından rastgele geliştirici buluşmalarına kadar, içgörülerle doludurlar.

GitHub? Büyük ödül.
Veritabanlarını ve Pastebin'i riske atmak mı? Her ikisi de bilgi paylaşımında son derece cömerttir.

Nmap ve Shodan? Kesinlikle güvenilir dostlarım, ancak açık sistemleri keşfetme konusunda en iyi yardımcılarım.

CVE veritabanı? Her zaman faydalıdır.

Gerçek tehdit istihbaratı beslemeleri? Bazıları değerli, bazıları ise önemsizdir–ancak etkili olanlar oyunun seyrini değiştirebilir.

Bu cephanelik (ve daha fazlası) ile, "sizin" – kim olduğunuz, nerede çalıştığınız, ne yaptığınız ve en önemlisi sizi bir şeye tıklamaya ya da bir sohbete katılmaya iten şeyin ne olduğu – tam bir profilini oluşturmak şaşırtıcı derecede kolaydır.

İlk Anlaşma: Size bu işe girmenin yollarını göstereyim.

Kimlik avı mı? Klasik bir yöntem. İkna edici bir e-posta ile gelen kutunuza sızacak ve her şeyi teslim etmenizi sağlayacağım.

Sosyal mühendislik mi? Telefonunuz, sohbetiniz veya hatta yüz yüze görüşmeniz aracılığıyla nazik bir dille size ulaşırım; inanın bana, bu oyunu nasıl oynayacağımı biliyorum.

Kimlik Bilgisi Doldurma? Şifrelerinizi tekrar mı kullanıyorsunuz? Harika. Sızdırılan kimlik bilgilerini alıp başka hangi sistemlere erişebileceğimi inceleyeceğim.

Kaba Kuvvet? Şifrelerinizi tahmin etmeye yönelik otomatik araçlarım mevcut–benim için uyku yok.

OTD BİLİŞİM
GLOBAL VAD

SmartDECEPTIVE

CATCHPROBE™

Sıfır Gün Saldırıları? Eğer henüz keşfedilmemiş bir güvenlik açığı varsa, bunu sizin aleyhinize kullanacak ilk kişi ben olacağım.

Truva atları mı? Meşru görünüyor, ancak içine kötü niyetli kodlar gizledim ve sizin yüklemenizi bekliyor.

Kimlik Bilgisi Doldurma? Şifrelerinizi tekrar mı kullanıyorsunuz? Harika. Sızdırılan kimlik bilgilerini alıp başka hangi sistemlere erişebileceğimi inceleyeceğim.

Kaba Kuvvet? Şifrelerinizi tahmin etmeye yönelik otomatik araçlarım mevcut—benim için uyku yok.

Fidye yazılımı mı? Dosyalarınızı kilitleyeceğim ve geri alabilmeniz için büyük bir meblağ talep edeceğim - ödemeniz sizin yararınıza olacaktır.

Aracı Adam mı? Eğer halka açık bir Wi-Fi kullanıyorsanız, farkında olmadan yaptığınız her şeyi dinleyebilirim.

SQL Enjeksiyonu nedir? O güvensiz web formları? Bunları veritabanınızın derinliklerine ulaşmak için kullanacağım.

Siteler Arası Komut Dosyası (XSS)? Bir web sayfasını yükleyeceksiniz ve kötü niyetli komut dosyaları, bilgilerinizi çalmak amacıyla yerleştirildi.

Uzaktan Kod Çalıştırma? Sisteminizde bir zafiyet mi tespit ettiniz? Harika, kötü niyetli kodumu uzaktan çalıştırarak kontrolü ele alacağım.

İstismar Kitleri? Zayıflıkları tarayıp otomatik olarak istismar etmek için hazır bir araç setim var - son derece basit.

Hadi canım, hepsini listelemem gerçekten gerekli mi?...

İçeri girdikten sonra yapacağım şey şu: İşletim sistemiymişim gibi davranarak antivirüs taleplerini engelleyeceğim, her yeni makineye bulaştığımda kodumu değiştireceğim ve gizli kalmak için kendimi yürütülebilir dosyaların içine şifreleyeceğim. Polimorfik bir motorla, her bulaşma sırasında kodumun önemli bölümlerini yeniden yazacağım ve eğer hırslı hissediyorsam, tamamen metamorfik hale gelip her hedef için kendimi tamamen yeniden yazacağım. Ardından, ağınızı tarayacak, DNS, DHCP ve sunucuları haritalayacak, ana bilgisayarlar arasındaki rotaları izleyecek ve MAC adreslerini kontrol edeceğim. Ayrıca bağlantılar için Netstat'ı ve adlar ile IP'ler için NBTStat'ı inceleyeceğim. Bunu yaptıktan sonra, tam olarak neyle karşı karşıya olduğumu görmek için DNS adlarını, NetBIOS adlarını, kullanıcı hesaplarını, MAC adreslerini, ağ bağdaştırıcılarını, paylaşımları ve hizmetleri sıralayacağım. Artık manzarayı bildiğime göre, bir sonraki hamlemi yapmak için tüm bu bilgileri kullanabilirim.

SmartDECEPTIVE

CATCHPROBE™

Uzlaşma: Bizi Durdurmak İçin Ne Yapabilirdiniz?

Güvenlik duvarları mı? Elbette, harikadırlar—tabii ki IoC'lerle aşırı yüklenmediğiniz sürece. (Hey... siz, evet siz, değerli müşterim, ThreatWAY'in alakasız IoC'leri filtrelediğini ve riskleri puanladığını bilmiyor musunuz? Böylece güvenlik duvarınız sizi bunaltmıyor!)

IDS/IPS? Baypass edildi. Alarmları devreye sokmadan nasıl geçeceğimizi biliyoruz.

DLP? Bir portu açık bıraktınız, değil mi? Verileri hemen aktaracağız. (RiskRoute'un o açık portları anında işaretleyeceğini bilselerdi!)

Derin Paket İncelemesi mi? Evet, 2012'den beri bunu atlatıyoruz.

Yamalar? Tüm satıcılarınızın güvenlik açıklarını izliyor musunuz? Sanırım bunu yapmıyorsunuz... (Şşş... DarkMAP bu konuda sizi koruyor.)

Antivirüs mü? Tebrikler, %3-7'lik etkinlik için—ah, ve zaten yarısının devre dışı bırakıldığı biliniyor.

SIEM? Yüklü mü? Harika. Ne yazık ki ekibiniz uyarılarda boğuluyor. (Evet... ThreatWAY ile değil—bunu küçük bir sır olarak saklayalım.)

Politikalar ve Prosedürler? Belki, eğer hepiniz bu konularda uzlaşabilir ve uygulama hususunda anlaşmazlık yaşamazsanız.

Gerçek şu ki, her zaman %100 kazanmanız gerekmektedir. Sadece bir kez şanslı olmamız yeterlidir.

Bu, güvenlik teknolojilerinizin güncelliğini yitirdiğini ifade etmekle ilgili değildir. Bu durum karmaşıktır, ancak çözümün yalnızca bir parçasını temsil eder. Son 20 yıldır güvenlik önlemeye odaklanılmıştır ve siber savaşı kazanmış değilsiniz. Şimdi, SaaS, IoT, BYOD, Bulut, V2V ve V2X ile çevreniz neredeyse gözenekli bir hale gelmiştir. Bu gelişen ortama uyum sağlayan akıllı ve tasarıma uygun çözümlere ihtiyacınız vardır. Tehdit modellerini ve niyetlerini tespit ederek saldırıları öngören çözümler; yemler, web istihbaratı, OSINT ve saldırganları anlamadan önce kavrayabilmek için eyleme geçirilebilir içgörüler gibi araçlar kullanır. Artık önleme tek başına yeterli olmayacaktır.