DIFOSE

GoSecure
Responder® PRO
Powered by Digital DNA®

Responder Pro

ÜRÜN HAKKINDA

Çoğu endpoint güvenlik aracı, sadece yüzeysel istihbarat toplar ve bu da genellikle olay müdahale uzmanlarına kötü amaçlı yazılımların sahip olabileceği daha geniş etkiyi anlamaya yetecek kadar bilgi sağlamaz.

GoSecure Responder PRO, tersine mühendislerin, belirli makinelerde kötü amaçlı yazılımın tam olarak nasıl yürütüldüğünü anlamalarına yardımcı olarak, sonuçları disassemble etme ve görselleştirmelerini sağlar. Dahası, tersine mühendislik işlemleriyle, tehditlerin nasıl nüfuz ettiğini anlamak ve yöneticilere diğer makineleri potansiyel olarak nasıl etkileyeceğini göstermek için kök nedene ilişkin ayrıntılı bilgi veren raporlar oluşturulabilir.

Responder PRO'nun kötü amaçlı yazılım analizi, amiral gemisi teknolojimiz olan Digital DNA®'ya dayanır. Hem 32 bit hem de 64 bit belleği analiz edebilir.

ÖZELLİKLER

GoSecure Responder PRO, kullanıcıların kötü amaçlı yazılım analizinde ve diğer tehdit göstergelerinde temel nedeni ortaya çıkarmasına yardımcı olan tescilli davranış motoru Dijital DNA'dan yararlanır. Temel fark, Responder PRO'nun, tek bir makinede gerçekleştirilen analizi ilişkilendirmek için 3000'den fazla özelliğe dayanan, sürekli güncellenen bir davranışsal zeka kaynağı sağlamasıdır.

Standart işlem ve modül ayrıntılarından açık dosyalar, soketler ve kayıt defteri anahtarları hakkındaki kapsamlı ayrıntılara kadar, fiziksel belleğin her öğesi, Responsder PRO ile analiz edilebilir.

Belge parçaları, internet geçmişi taranabilir, anahtar ve şifreler otomatik olarak bellekten çıkarılır ve kullanılabilir hale getirilir.

AÇIKLAMALAR

CANLI BELLEKTE BULUNAN BİLGİ TÜRLERİ

İşletim sistemi bilgileri:

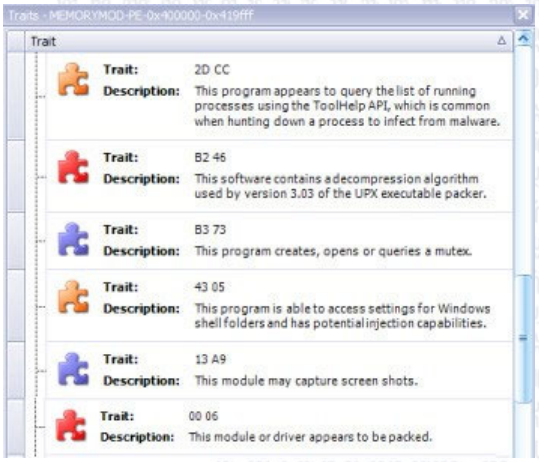
- Çalışan süreçler ve modüller
- Açık dosyalar
- Ağ bağlantıları ve dinleme bağlantı noktası
- Açık kayıt defteri anahtarları
- Kesinti Tanımlayıcı Tablosu
- Sistem Hizmetleri Tanımlayıcı Tablosu

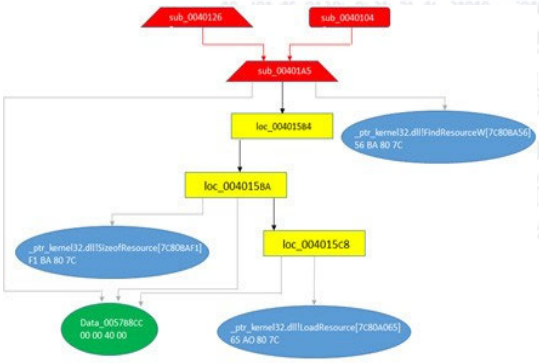
Uygulama bilgileri:

- Açık metin olarak şifre
- Şifrelenmemiş veriler
- Anında mesajlaşma sohbet oturumları
- Belge verileri
- Web tabanlı e-posta
- Outlook e-posta

Kötü Amaçlı Yazılım Algılama:

- Keylogger'lar
- Rootkit'ler
- Truva atları
- Botlar
- Bankacılık Truva Atları
- Polimorfik kod





Dijital DNA® ile Kötü Amaçlı Yazılım Tespiti Daha Kolay

GoSecure'un patentli bellek analizi teknolojisi olan Digital DNA® ile, Responder PRO bellek görüntülerinde otomatik olarak tersine mühendislik yapar ve kötü niyetli amaç açısından inceler. Gözlemlenen davranış özellikleri, dijital nesneleri iyi, kötü veya nötr olarak sınıflandırmak için GoSecure'ün Kötü Amaçlı Yazılım Genomu veritabanıyla eşleştirir. Kapsamlı bir tehdit profilinin parçası olarak sunulan genel önem derecesini hesaplamak için kurallar ve puanlama uygulanır.

GoSecure, siber güvenlik çözümlerinde lider ve yenilikçi olarak tanınmaktadır. Şirket, Uç Nokta ve Ağ tehdit algılama platformunu, Yönetilen Tespit ve Yanıt hizmetlerini ve Bulut / SaaS dağıtımını entegre eden ilk ve tek şirkettir. Bu yetenekler ile birlikte, insanları, süreçleri ve sistemleri hedefleyen sürekli gelişen kötü amaçlı yazılımların ve içerideki kötü niyetli kişilerin artan karmaşıklığına en etkili yanıtı verir.

Grafik ve Raporlama

GoSecure Responder PRO Canvas görünümü, kötü amaçlı yazılım parçasını oluşturan öğelerin sistemin diğer bölümlerine nasıl bağlandıklarının etkileşimli bir grafik penceresini sağlar. Kanvas grafikler, yürütme dallarını izole etmenize veya bağlamanıza, işlevleri daraltmanıza, genişletmenize ve ham verilerin ilgili bölümlerine atlamanıza olanak tanıyarak program davranışlarını izlemek için somut bir model sunar.

Kullanım kolaylığı için tasarlanan Responder PRO raporları, bir bakışta kritik tehdit istihbaratı sağlar.

Ankara: Ümit Mah. 4281 Sok. Kafkas Sitesi No:6 06810 Ümitköy/ÇANKAYA
İstanbul: Esentepe Mah. Kelebek Sk. No:2 Marmara Kule Kat:10 D:79 34870 KARTAL
+90 (312) 219 56 16
+90 (216) 771 07 97