



GOSECURE

Digital DNA®



ÜRÜN HAKKINDA

Digital DNA®, fikri mülkiyet hırsızlığı, sınıflandırılmış bilgiler ve müşteri kayıtlarını ele geçirmek amacıyla küresel boyutta kullanılanlar da dahil olmak üzere en gelişmiş zararlı yazılım tehditlerini tespit etmek için bir endpoint belleğini adli bilişim bakış açısıyla analiz eden davranış analizi teknolojisidir.



DİJİTAL DNA'NIN GÜCÜ

Benzersiz adli bilişim ve patentli DNA teknolojisi, günümüzün en gizli kötü amaçlı yazılımları tarafından kullanılan çok çeşitli anti-adli inceleme önlemlerini tespit eder ve ortadan kaldırır. Otomatik analiz sayesinde bir tehdit belirlendikten sonra, bu tehdidin yetenekleri hakkında hızlı bilgi toplanır ve diğer potansiyel tehlike altındaki sistemleri saptamanıza, ilk bulaşma noktalarını belirlemenize ve kalan kötü amaçlı dosyaları ve sistem değişikliklerini izole etmenize olanak tanır.



NASIL ÇALIŞIR

Dijital DNA, bellekteki tüm kodlarda otomatik olarak tersine mühendislik yapar ve imza, IOCS veya buluşsal yöntemlere dayanmadan kötü amaçlı yazılım davranışını belirlemek için her bir modülü eşlemeye çalışır. Davranışlar, CounterTack'in Kötü Amaçlı Yazılım Genomu veritabanındaki özelliklerle eşleştirilir ve iyi, kötü veya nötr olarak sınıflandırılır.

Dijital DNA, fiziksel belleğe doğrudan erişerek ve her modülün belirli davranış özelliklerini belirleyerek, zero day, root kit ve hedefli saldırılar dahil olmak üzere bilinen birçok sistemin kaçırdığı çok sayıda yeni kötü amaçlı yazılımı güvenilir bir şekilde algılar.





ETKİNLİK TESTİ

CounterTack, daha önce görülmemiş tehditlerin başarılı bir şekilde tespit edilmesini sağlamak için Dijital DNA'nın sürekli etkinlik testini gerçekleştirir. Her test turu için, üçüncü taraf beslemelerinden rastgele 25.000 kötü amaçlı dosya seçilir ve taranır. Dijital DNA şu anda bilinmeyen tehditler için % 93 pozitif tespit oranına sahiptir.

COUNTERTACK'S ACTIVE DEFENSE İÇİN DIGITAL DNA

Active Defense, ham fiziksel belleği, canlı işletim sistemini ve NTFS birimlerini merkezi bir konsoldan taramanıza olanak tanıyan kurumsal çapta bir Dijital DNA yönetim çözümüdür. Bir tehdit belirlendikten sonra, otomatik toplama ve analiz yetenekleriyle olaya müdahalesini düzene sokarak ekibinizin çabalarını on binlerce veya yüz binlerce sisteme göre ölçeklendirmesine olanak tanır.

Process Name	Module Name	Path	PID	Score	Viewed	Discovered On	Hash Set	Actions
badware.exe	junkdriver.sys	\\?c:\windows\system32\drivers	3,236	113.8		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄
svchost.exe	kernel.dll	\\windows\system32	2,452	60.8		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄
explorer.exe	kernel.dll	\\windows\system32	2,452	45.1		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄
svchost.exe		[Unknown]	2,452	24.8		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄
procmon.exe	procmon.exe	c:\tools\procmon	660	23.8		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄
SYSTEM	procmon23.sys	\\?c:\windows\system32\drivers	4	22.2		7/17/2014 17:06	[None]	🔍 🔄 🗑️ 📄

Dijital DNA teknolojisiyle desteklenen Active Defense, endpoint belleğinin anlık görüntüsünü adli olarak tarar ve yürütülebilir kodun tehdit şiddetini derecelendirmek için Dijital DNA kullanır.



COUNTERTACK RESPONDER® PRO İÇİN DIJITAL DNA

Responder PRO, Windows® ve Linux fiziksel bellek edinimi ve analizi için bir endüstri standardıdır. Responder PRO, yalnızca birkaç tıkla, canlı bellekteki kötü amaçlı yazılımları algılar, yeteneklerini sıralar ve olay müdahalesi, veri uyumluluğu ve elektronik keşif için kritik olan yapıları ortaya çıkarır. Responder PRO ile olay müdahale ekibiniz herhangi bir siber tehdidi kolayca anlayabilir ve buna karşı ağ savunmasını hızla güçlendirebilir.

Digital DNA Sequence	Name	Process Name	Size	Severity	Weight
04D3C5014DF2011E7B008C160...	MEMORYMOD-PE-0x400000-0x...	svchost.exe	106496		85.0
00C7C50F2022006609000E6F0...	MEMORYMOD-PE-0x3870000-0...	svchost.exe	450560		44.2
005D09025FCE01685A0385AD...	ieframe.dll	ieexplore.exe	11010048		31.6
005D0901685A011E7B008C160...	ieframe.dll	ieexplore.exe	11010048		26.8
2180AC005A6A008C16006609...	wuaueng.dll	svchost.exe	2437120		25.8
005A6A008C160066090015490...	TPSvc.dll	tpautoconnect.exe	692224		25.1



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