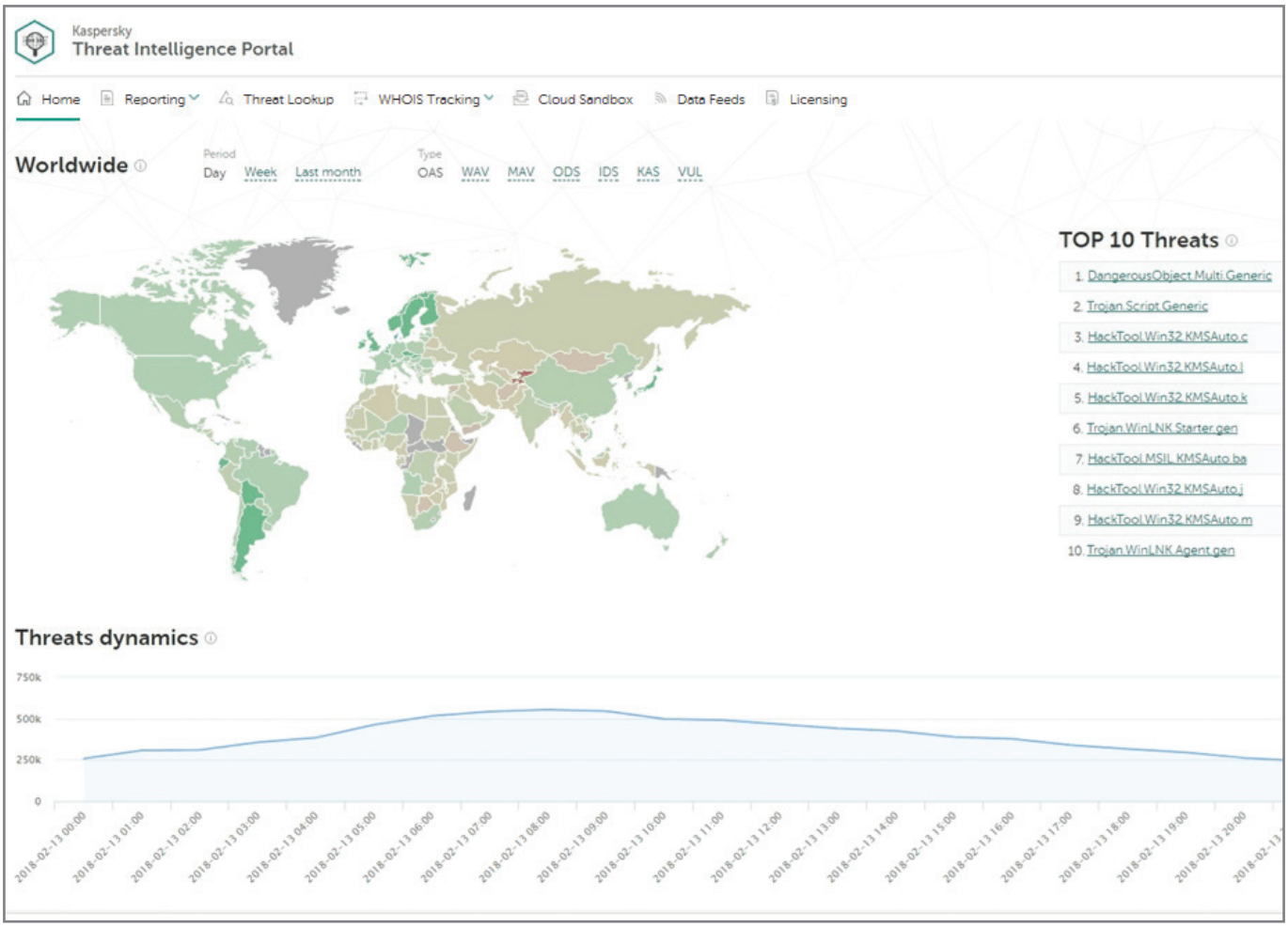
KASPERSKY lab

Kaspersky Tehdit İstihbaratı Portalı: Olay İncelemesi ve Yanıtı

www.kaspersky.com.tr/fraudprevention
#truecybersecurity

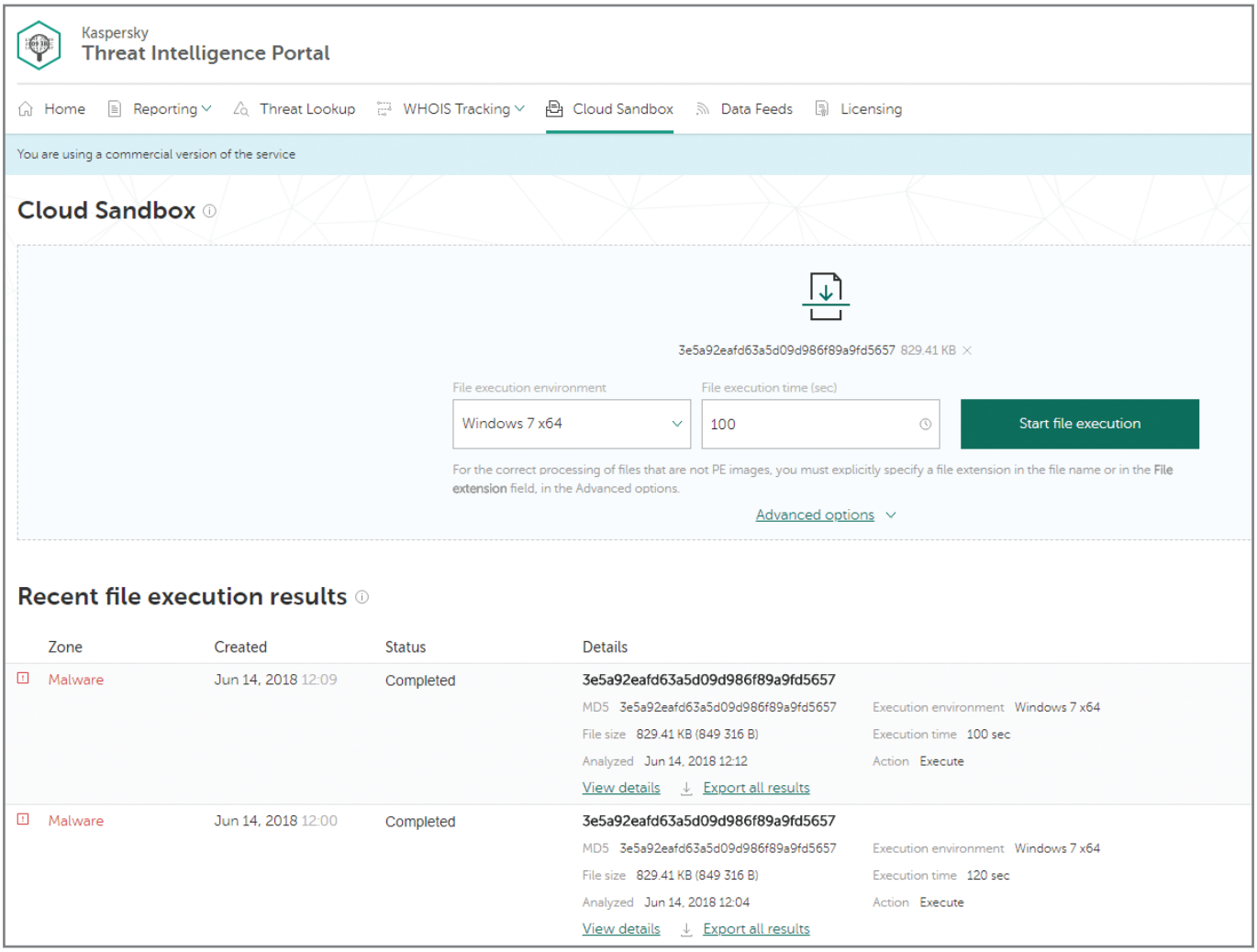
Kaspersky Tehdit İstihbarat Portalı, Kaspersky Lab'in yirmi yılı aşkın şirket geçmişi üzerinde topladığı, geliştirdiği ve kategorize ettiği tüm bilgileri sunar. Platform; olaylar, URL'ler, etki alanları, IP adresleri, dosya karmaları, tehdit adları, istatistiksel/davranış verileri, WHOIS/DNS verileri vb. hakkında en son ayrıntılı tehdit bilgilerini alır ve olay yanıt ekiplerinin aşağıdaki işlemleri yapmasına olanak verir:

- Sıradaki bir olayın derhal yanıt mı yoksa ekstra inceleme mi gerektirdiğini belirleme
- Bir olayın tam kapsamını belirlemek ve buna uygun olarak yanıt vermek için ilk algılamayı başlangıç noktası olarak kullanma
- Kimlerin etkilendiğini, neyin etkilendiğini ve etkinin ne olduğunu tanımlama ve diğer ilgili departmanlara anlamlı bilgiler sağlama
- En etkili yanıtı belirlemek için siber suçluların kullandığı taktikleri, teknikleri ve hedefleri anlama

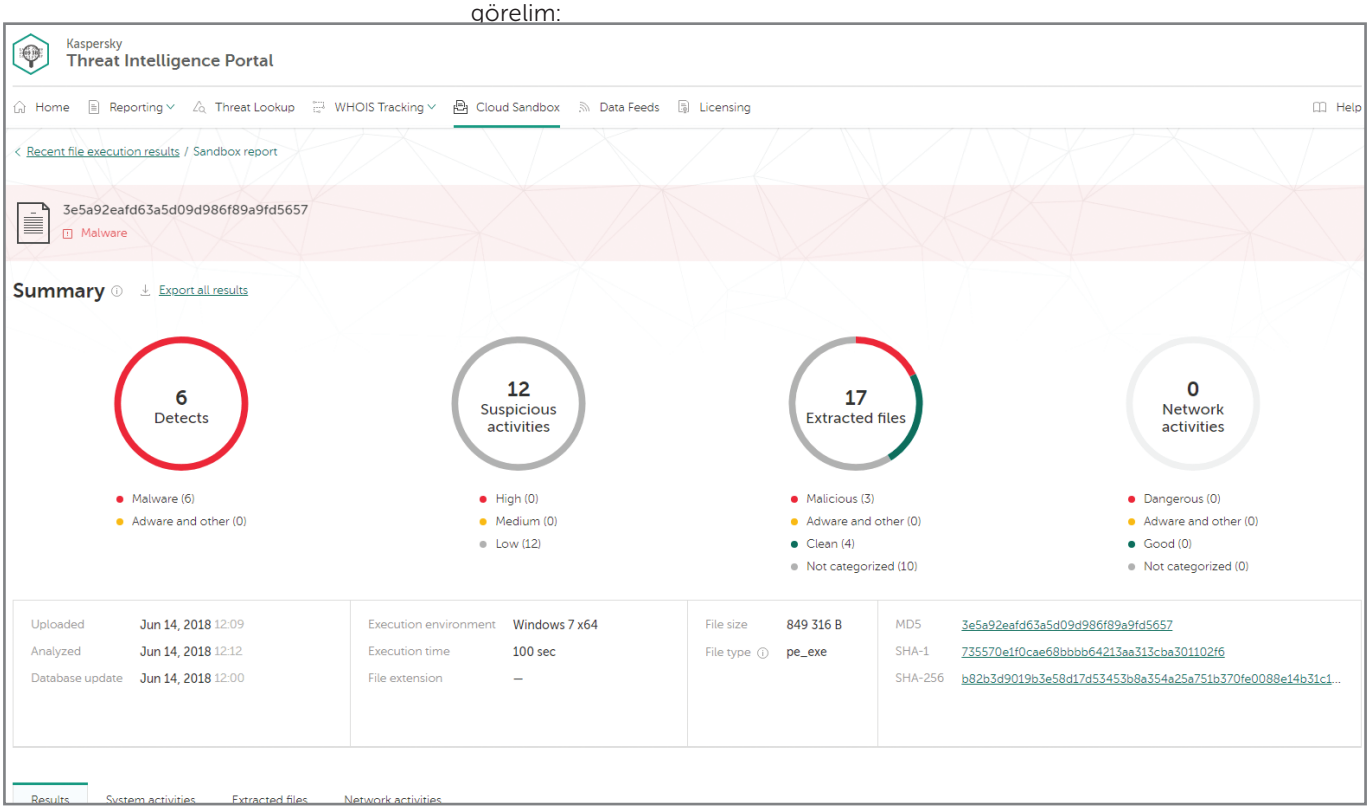


Tehdit İstihbarat Portalı ana sayfasında çok sayıda sekme vardır, ancak bu örnek için, canlı kanıtlara sahip olduğumuzu düşünelim. Olay müdahale ekibi, normal çalışma saatleri dışında harici bir IP adresi ile ağ çevresinin içinden iletişim başlatan şüpheli bir dosya örneği elde ediyor. Bu durumda, üst menüdeki Cloud Sandbox sekmesine doğrudan gidebilirsiniz.

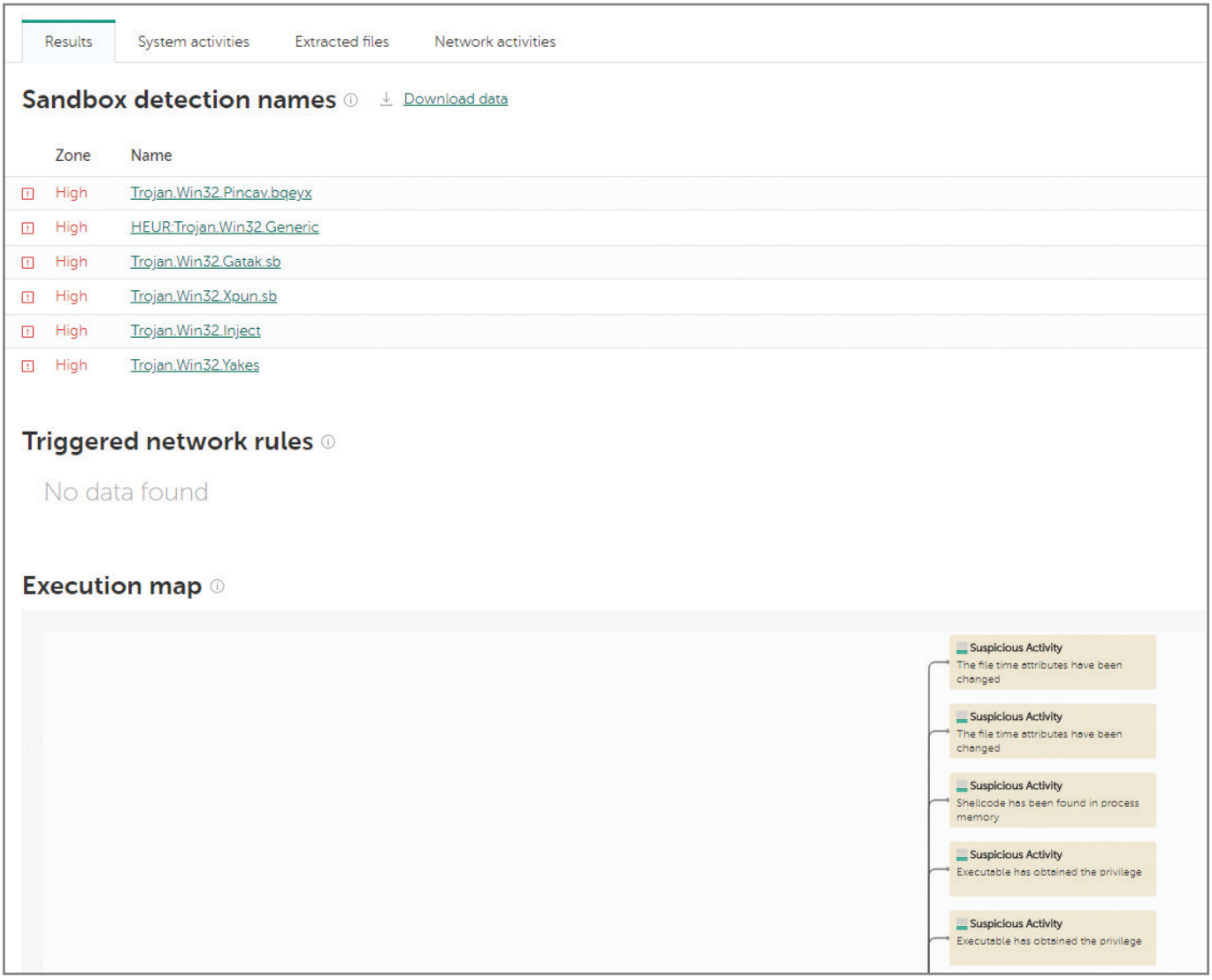
Korumalı alan, tam özellikli bir işletim sistemi olan bir sanal makinede (VM) şüpheli bir nesne çalıştırır. Davranışını analiz ederek bir nesnenin kötü amaçlı etkinliğini tespit eder. VM'ler gerçek işletme altyapısından izole edilir, bu nedenle böylesi bir açılma gerçek hasara neden olmaz. Dosyanızı yükleyin, ortamı seçin (bu durumda Windows 7), süreyi seçin (mesela 100 saniye) ve yürütme işlemini başlatın:

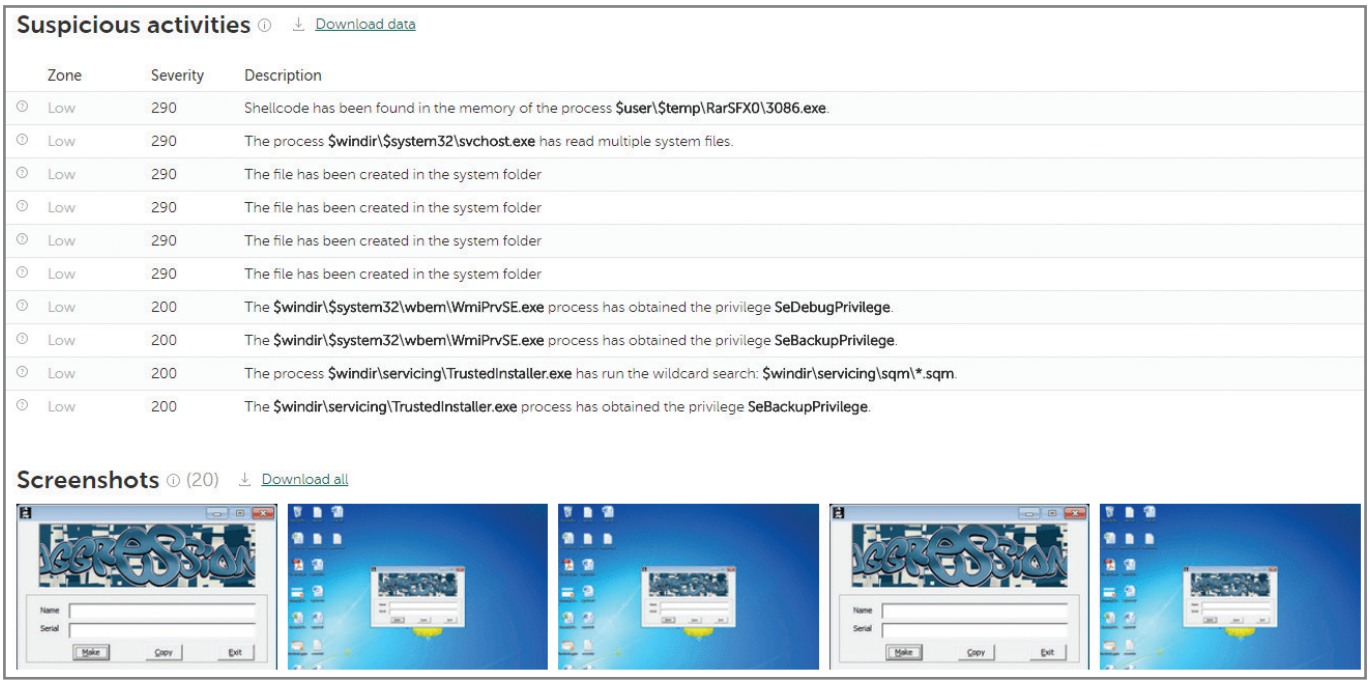


Korumalı alan, statik analizden kurtulan kötü amaçlı yazılımlara karşı etkilidir — bu nedenle antivirüsünüz, şüpheli bir dosyayı tamamen kaçırmış olabilir. Bu dosya "kötü" olarak tanımlansa dahi, çoğu antivirüs sistemi dosyanın ne kadar kötü olduğunu veya gerçekte ne olduğunu açıklamaz. Daha fazla ayrıntı elde etmek için, açılma sonrasında Kaspersky Cloud Korumalı Alan'da neler olduğunu görelim:



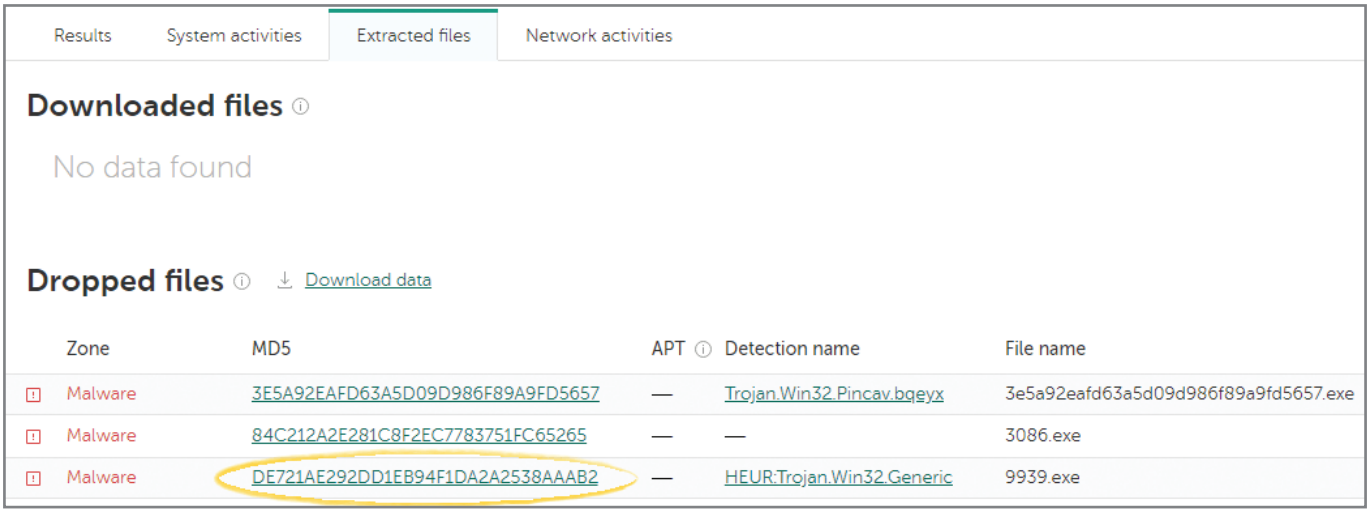
Bir koruma alanı test edilen nesneyi çalıştırarak yapay nesneleri analiz eder ve vardığı sonucu iletir. Özet şu şekildedir: algılamalar (6), şüpheli etkinlikler (12), ayıklanan dosyalar (17) ve ağ etkinlikleri (0). Görüldüğü gibi dosya yalnızca bir "kötü" dosya olmanın ötesindedir; bu dosya pek çok kötü eylem gerçekleştirir ve bunların hepsi listelenir.





Sonuçlar sekmesinde, bir olay yanıt ekibi yürütme sırasında alınan ekran görüntülerini görebilir. Bazı durumlarda, kötü amaçlı yazılım kullanıcı etkileşimini (bir parola girerek, belge üzerinde gezinerek, fareyi hareket ettirerek vb.) bekleyerek otomatik analiz yapmaya çalışır. Kaspersky Cloud Korumalı Alan, birçok kaçınma tekniğini bilir ve bu tekniklere karşı koymak için insan odaklı teknolojiler kullanır. Ekran görüntüleri de bu konuda yararlı olabilir: Bir araştırmacı, bir insan bakış açısından "test tüpünde" neler döndüğünü görebilir.

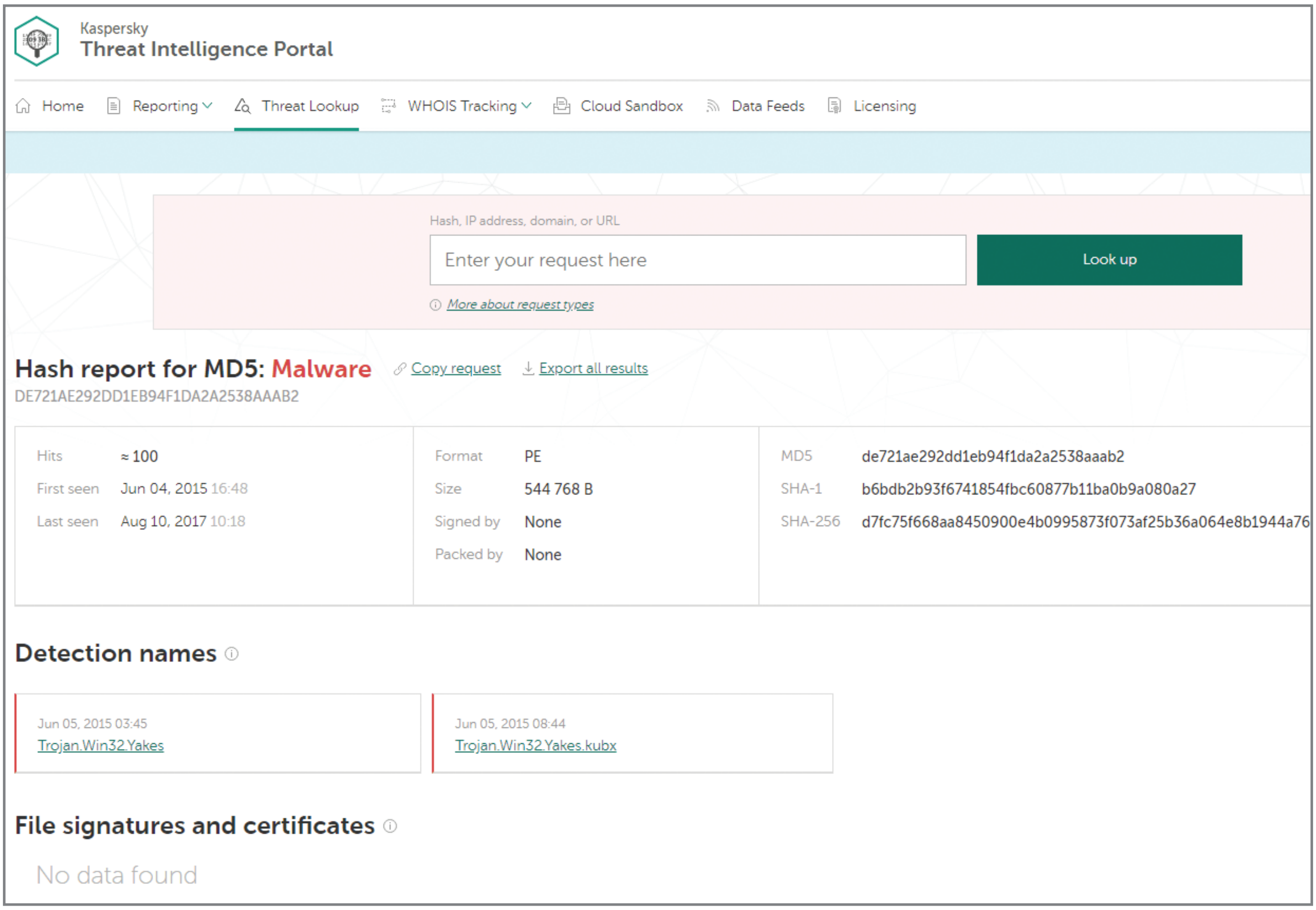
Karşıdan yüklenen, ayıklanan veya bırakılan nesneleri görmek için Ayıklanan dosyalar sekmesine geçelim. Bu senaryoda, kötü amaçlı bir dosya bırakılmıştır:



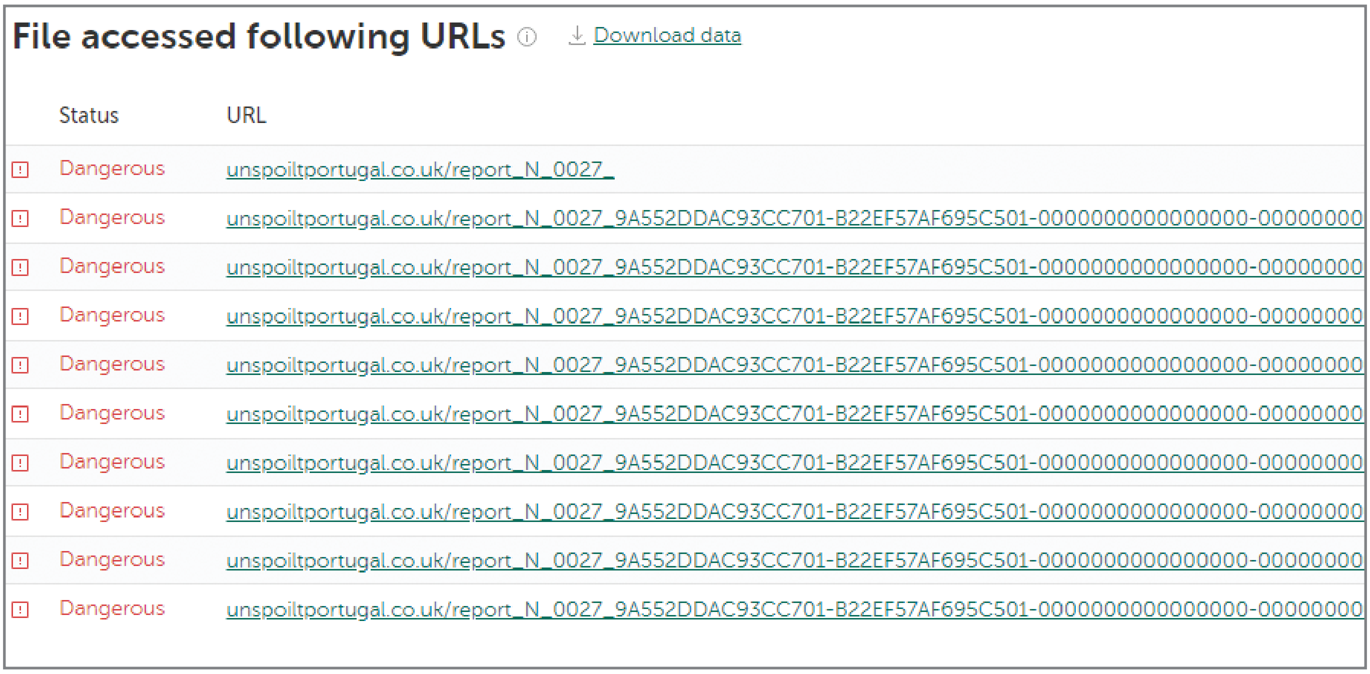
Klasik korumalı alan özellikleri bu noktada sona erer: dosyayı çalıştırdınız ve kötü niyetli etkinlikler listesini edindiniz. Hepsi bu kadardır. Ancak Kaspersky Tehdit İstihbaratı Portalı ile, risk göstergeleri ve ilişkileri hakkında daha ayrıntılı bilgi almak için doğrudan Thread Lookup (Tehdit Arama) kısmına geçebilirsiniz.

Tehdit Arama, güvenliğe yönelik arama motorumuzdur. Kaspersky Lab tarafından son 20 yılda toplanan ve kategorize edilen yaklaşık 5 petabayt tehdit istihbaratı içerir: dosya karmaları, istatistiksel/davranış verileri, WHOIS/DNS verileri, URL'ler, IP adresleri vb.

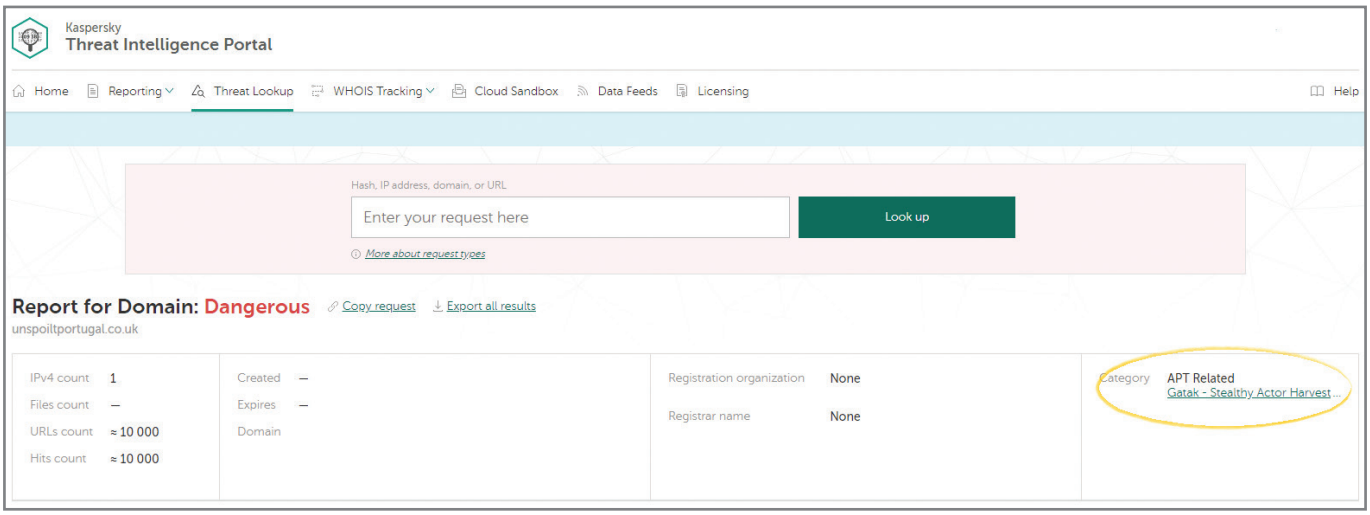
Bu nedenle, korumalı alanda örneğimizi çalıştıktan sonra, yalnızca nesneye tıklayarak (bu senaryoda MD5 karması) Tehdit Arama için arama sorguları olarak koruma sonuçlarını kullanırız.



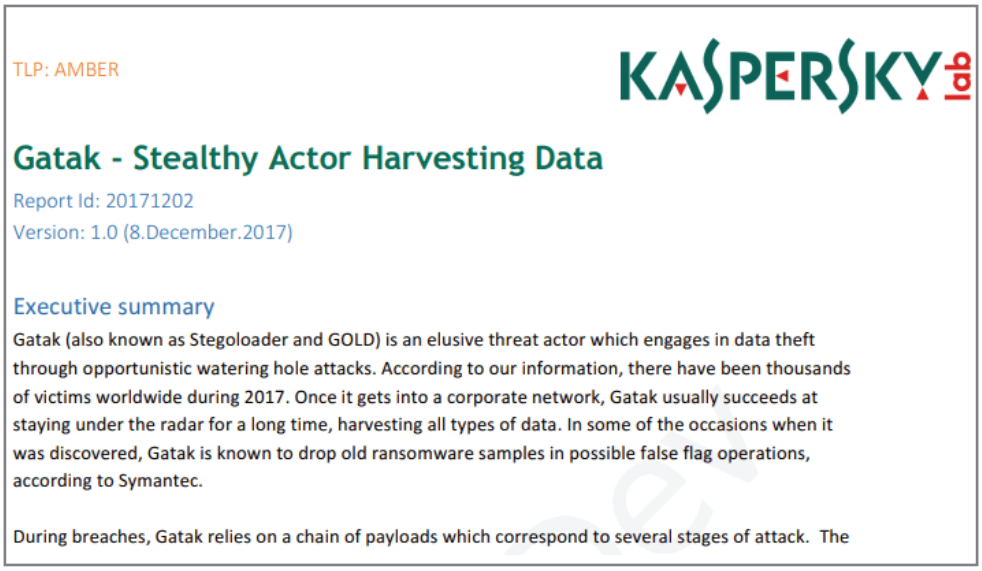
Şimdi kötü amaçlı yazılımlar hakkında daha ayrıntılı bir raporumuz var. Şimdi keşfettiğimiz zararlı yazılımlar tarafından hangi URL'lere erişildiğini görmek için Tehdit Arama sonuçları kısmına bakalım:



İşte “Tehlikeli” olarak işaretlenmiş bir URL. Tehdit Arama hizmetimizde bu URL hakkında ne yazdığını görmek için bu kötü amaçlı URL'ye göz atalım:



Görüşüne göre söz konusu kötü amaçlı URL, bir APT saldırısı ile ilişkili! Kaspersky Tehdit İstihbarat Portalı bir APT raporunu indirmeyi önerecektir. Bu PDF'de bir yönetici özeti, ayrıntılı teknik ayrıntılar ve ilgili bir risk göstergesi listesi bulunmaktadır. Kurumunuzda benzer herhangi bir şeyin yaşanıp yaşanmadığını kontrol etmek ve açıklanan saldırının tespit edilmesi için belirli kullanım senaryolarını zamanında geliştirmek için bu dosyayı incelemek faydalı olacaktır.


TLP: AMBER

KASPERSKY lab

Gatak - Stealthy Actor Harvesting Data

Report Id: 20171202
Version: 1.0 (8.December.2017)

Executive summary

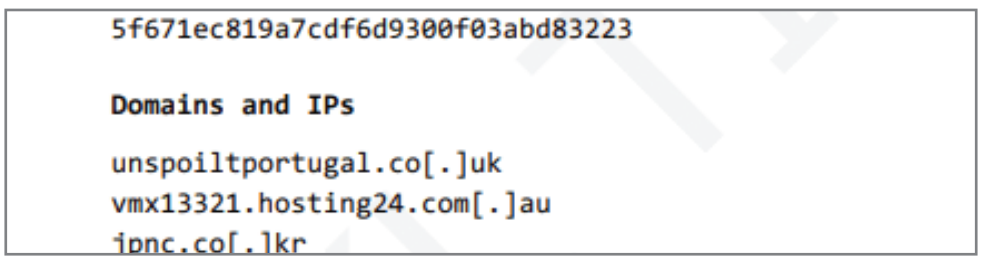
Gatak (also known as Stegoloader and GOLD) is an elusive threat actor which engages in data theft through opportunistic watering hole attacks. According to our information, there have been thousands of victims worldwide during 2017. Once it gets into a corporate network, Gatak usually succeeds at staying under the radar for a long time, harvesting all types of data. In some of the occasions when it was discovered, Gatak is known to drop old ransomware samples in possible false flag operations, according to Symantec.

During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The


Appendix I - Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473


5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoiltportugal.co[.]uk
vmx13321.hosting24.com[.]au
jpnc.co[.]kr

Kaspersky Tehdit İstihbarat Portalı ile şunları yapabilirsiniz:

- Olay yanıtınızı ve adli inceleme kabiliyetlerinizi geliştirir ve hızlandırır: Güvenlik/Güvenlik İşlemleri Merkezi ekibinizin, hedefli tehditlerin arkasında yatan nedenleri anlaması için tehditler ve global veriler hakkında anlamlı bilgiler sunar. Ana bilgisayardaki ve ağdaki güvenlik olaylarını daha verimli ve etkili bir şekilde teşhis eder ve analiz eder; olay yanıtı süresini en aza indirmek ve kritik sistemler ve veriler tehlikeye girmeden ölüm zincirini durdurmak için bilinmeyen tehditlere karşı iç sistemlerden gelen sinyalleri önceliklendirir.

- Tehdit göstergelerini derinlemesine araştırır. IP adresleri, URL'ler, etki alanları veya dosya karmaları gibi tehdit göstergelerini son derece güvenilir tehdit bağlamı içerisinde araştırır. Bu sayede saldırıları önceliklendirmenizi, personele doğru görevlerin verilmesini ve işletmeniz için en büyük riski oluşturan tehditlere odaklanmanızı sağlar.

- Hedefli saldırıların riskini azaltır. Kurumunuzun karşılaştığı belirli tehditlere karşı mücadele için savunma stratejileri geliştirerek taktiksel ve stratejik tehdit istihbaratıyla güvenlik tutumunuzu geliştirir.

Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr