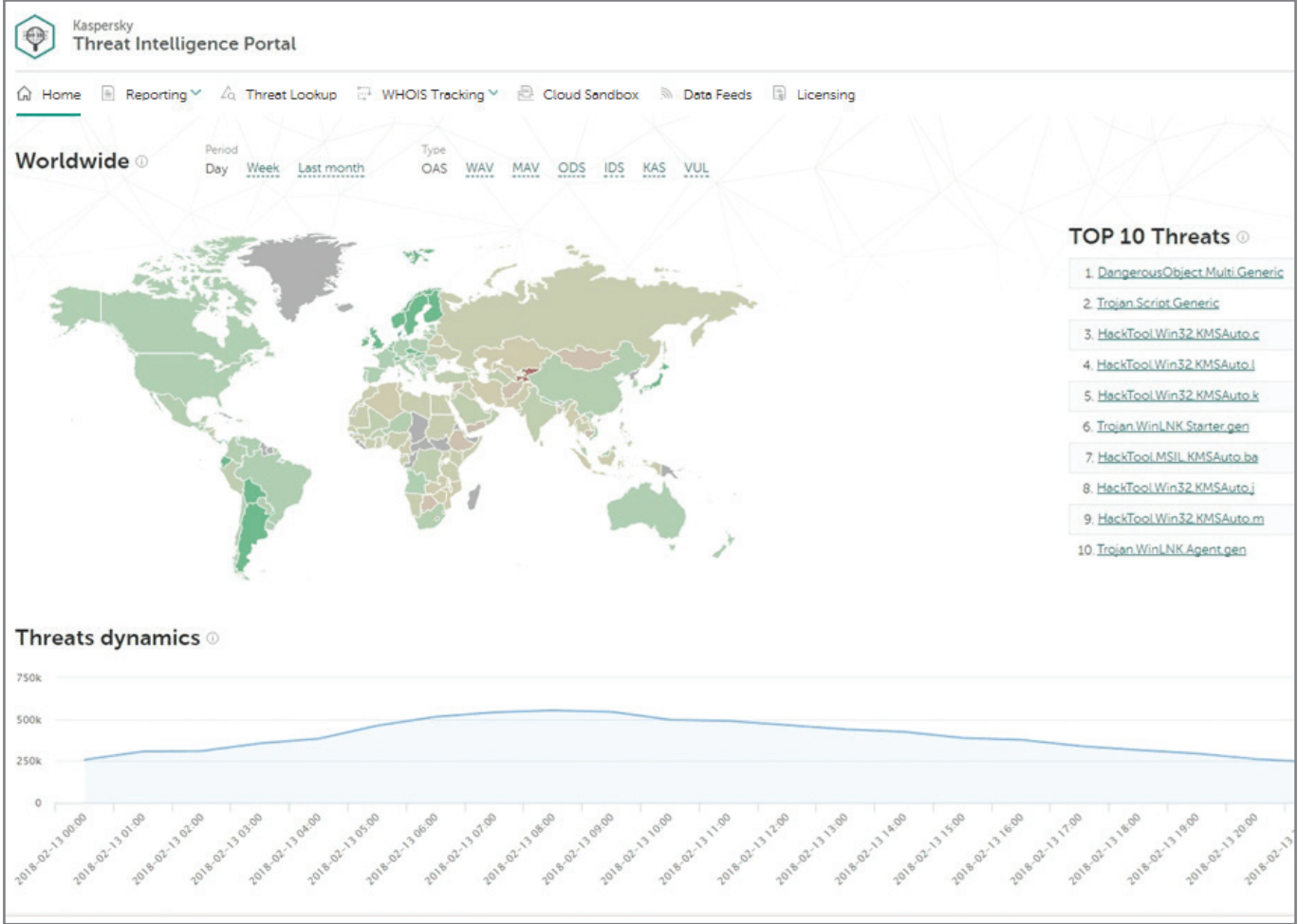


Kaspersky Tehdit İstihbaratı Portalı: Olay İncelemesi ve Yanıtı

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:

Kaspersky
Threat Intelligence Portal

Home
Reporting
Threat Lookup
WHOIS Tracking
Cloud Sandbox
Data Feeds
Licensing

You are using a commercial version of the service

Cloud Sandbox

3e5a92eafd63a5d09d986f89a9fd5657 829.41 KB

File execution environment
Windows 7 x64

File execution time (sec)
100

Start file execution

For the correct processing of files that are not PE images, you must explicitly specify a file extension in the file name or in the File extension field, in the Advanced options.

[Advanced options](#)

Recent file execution results

Zone	Created	Status	Details
Malware	Jun 14, 2018 12:09	Completed	3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 100 sec Analyzed Jun 14, 2018 12:12 Action Execute View details Export all results
Malware	Jun 14, 2018 12:00	Completed	3e5a92eafd63a5d09d986f89a9fd5657 MD5 3e5a92eafd63a5d09d986f89a9fd5657 Execution environment Windows 7 x64 File size 829.41 KB (849 316 B) Execution time 120 sec Analyzed Jun 14, 2018 12:04 Action Execute View details Export all results

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:

Kaspersky
Threat Intelligence Portal

Home
Reporting
Threat Lookup
WHOIS Tracking
Cloud Sandbox
Data Feeds
Licensing
Help

< Recent file execution results / Sandbox report

3e5a92eafd63a5d09d986f89a9fd5657
Malware

Summary

6
Detects

12
Suspicious activities

17
Extracted files

0
Network activities

Malware (6)
Adware and other (0)

High (0)
Medium (0)
Low (12)

Malicious (3)
Adware and other (0)
Clean (4)
Not categorized (10)

Dangerous (0)
Adware and other (0)
Good (0)
Not categorized (0)

Uploaded	Jun 14, 2018 12:09	Execution environment	Windows 7 x64	File size	849 316 B	MD5	3e5a92eafd63a5d09d986f89a9fd5657
Analyzed	Jun 14, 2018 12:12	Execution time	100 sec	File type	pe_exe	SHA-1	735570e1f0cae68bbb64213aa313cba301102f6
Database update	Jun 14, 2018 12:00	File extension	—			SHA-256	b82b3d9019b3e58d17d53453b8a354a25a751b370fe0088e14b31c1...

Results
System activities
Extracted files
Network activities

Bir koruma alanı test edilen nesneyi çalıştırarak yapay nesneleri analiz eder ve verdiği 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.

Results System activities Extracted files Network activities

Sandbox detection names [Download data](#)

Zone	Name
High	Trojan.Win32.Pincav.bqeyx
High	HEUR:Trojan.Win32.Generic
High	Trojan.Win32.Gatak.sb
High	Trojan.Win32.Xpun.sb
High	Trojan.Win32.Inject
High	Trojan.Win32.Yakes

Triggered network rules [Download data](#)

No data found

Execution map [Download data](#)

- Suspicious Activity: The file time attributes have been changed
- Suspicious Activity: The file time attributes have been changed
- Suspicious Activity: Shellcode has been found in process memory
- Suspicious Activity: Executable has obtained the privilege
- Suspicious Activity: Executable has obtained the privilege

Suspicious activities [Download data](#)

Zone	Severity	Description
Low	290	Shellcode has been found in the memory of the process \$user\temp\RarSFX0\3086.exe.
Low	290	The process \$windir\system32\svchost.exe has read multiple system files.
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	290	The file has been created in the system folder
Low	200	The \$windir\system32\wbem\WmiPrvSE.exe process has obtained the privilege SeDebugPrivilege.
Low	200	The \$windir\system32\wbem\WmiPrvSE.exe process has obtained the privilege SeBackupPrivilege.
Low	200	The process \$windir\servicing\TrustedInstaller.exe has run the wildcard search: \$windir\servicing\sqm*.sqm.
Low	200	The \$windir\servicing\TrustedInstaller.exe process has obtained the privilege SeBackupPrivilege.

Screenshots [Download all](#)

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:

Results

System activities

Extracted files

Network activities

Downloaded files ⓘ

No data found

Dropped files ⓘ

Download data

Zone	MD5	APT ⓘ	Detection name	File name
ⓘ Malware	3E5A92EAFD63A5D09D986F89A9FD5657	—	Trojan.Win32.Pincav.bqeyx	3e5a92eafd63a5d09d986f89a9fd5657.exe
ⓘ Malware	84C212A2E281C8F2EC7783751FC65265	—	—	3086.exe
ⓘ Malware	DE721AE292DD1EB94F1DA2A2538AAAB2	—	HEUR:Trojan.Win32.Generic	9939.exe

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 çalıştırdıktan sonra, yalnızca nesneye tıklayarak (bu senaryoda MD5 karması) Tehdit Arama için arama sorguları olarak koruma sonuçlarını kullanırız.



Hash, IP address, domain, or URL

Enter your request here

Look up

[More about request types](#)

Hash report for MD5: **Malware** [Copy request](#) [Export all results](#)

DE721AE292DD1EB94F1DA2A2538AAAB2

Hits	≈ 100	Format	PE	MD5	de721ae292dd1eb94f1da2a2538aaab2
First seen	Jun 04, 2015 16:48	Size	544 768 B	SHA-1	b6bdb2b93f6741854fbc60877b11ba0b9a080a27
Last seen	Aug 10, 2017 10:18	Signed by	None	SHA-256	d7fc75f668aa8450900e4b0995873f073af25b36a064e8b1944a76
		Packed by	None		

Detection names

Jun 05, 2015 03:45 Trojan.Win32.Yakes	Jun 05, 2015 08:44 Trojan.Win32.Yakes.kubx
--	---

File signatures and certificates

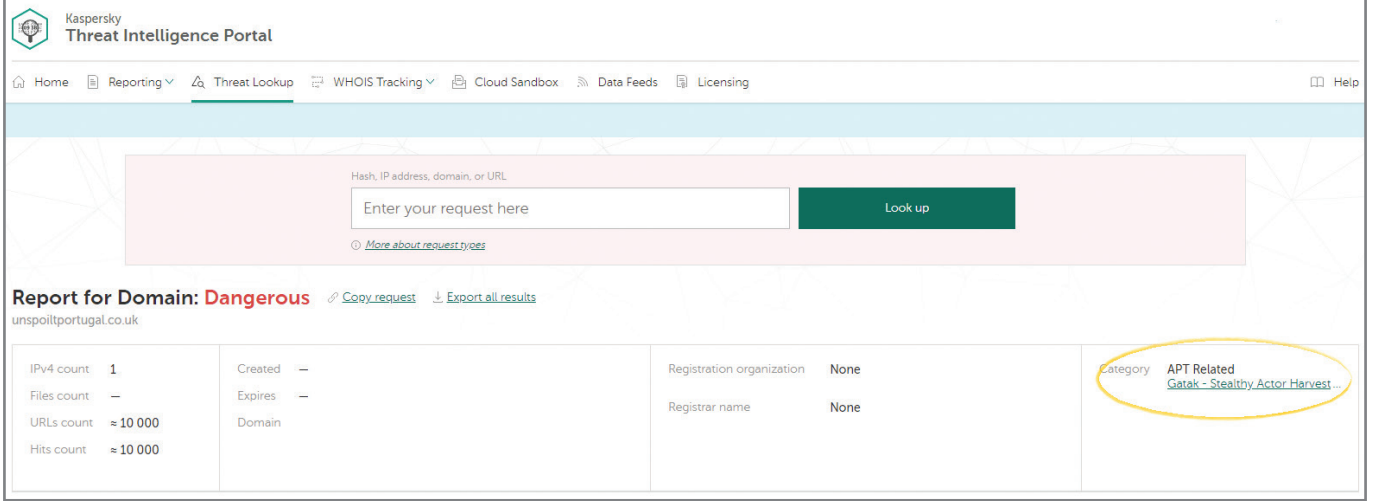
No data found

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:

File accessed following URLs [Download data](#)

Status	URL
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000
Dangerous	unspoilportugal.co.uk/report_N_0027_9A552DDAC93CC701-B22EF57AF695C501-0000000000000000-00000000

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



Kaspersky Threat Intelligence Portal

Home Reporting Threat Lookup WHOIS Tracking Cloud Sandbox Data Feeds Licensing Help

Hash, IP address, domain, or URL

Enter your request here

Look up

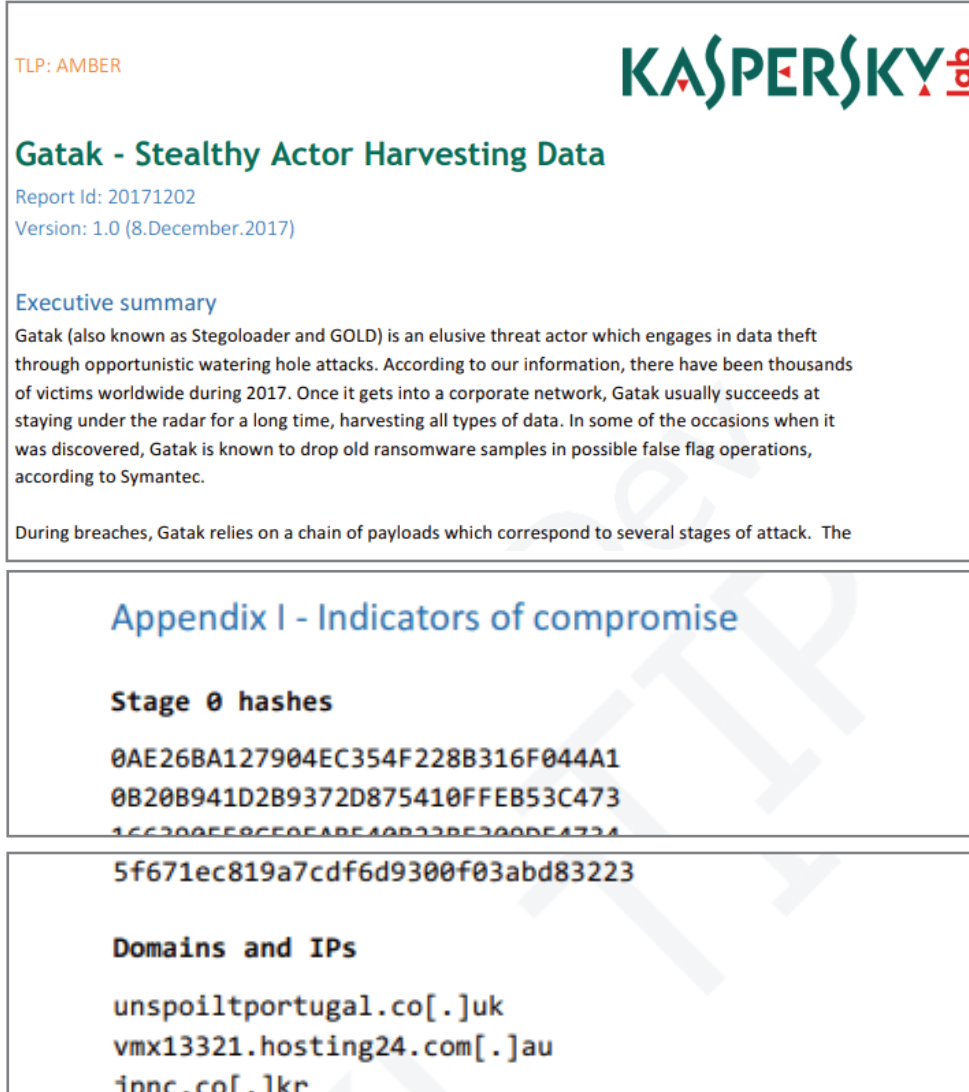
[More about request types](#)

Report for Domain: Dangerous [Copy request](#) [Export all results](#)

unspoilportugal.co.uk

IPv4 count: 1	Created: —	Registration organization: None	Category: APT Related
Files count: —	Expires: —	Registrar name: None	Gatak - Stealthy Actor Harvesting Data
URLs count: ≈ 10 000	Domain: —		
Hits count: ≈ 10 000			

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
166200F5F8C50FABE40B22BE200DE4724
5f671ec819a7cdf6d9300f03abd83223

Domains and IPs

unspoilportugal.co[.]uk
vmx13321.hosting24.com[.]au
ipnc.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 Güvenlięiyle İlgili Haberler: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com.tr

© 2019 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları, ilgili sahiplerinin mülkiyetindedir.

