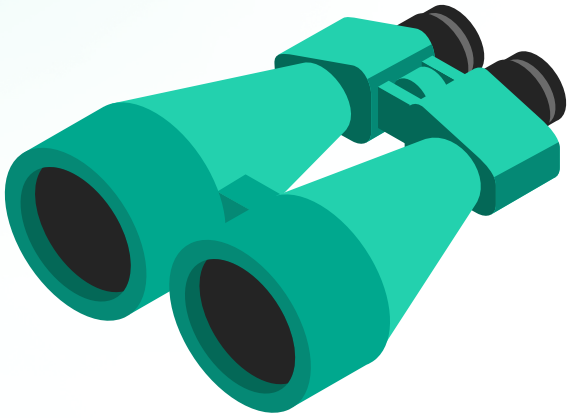
Managed Detection and Response: Analyst Report

Q4 2020



kaspersky

Samenvatting

* Kritiek: incidenten met grote impact die samenhangen met aanvallen met menselijke tussenkomst; deze vormen 9%* van alle geïdentificeerde incidenten

Aanbevelingen

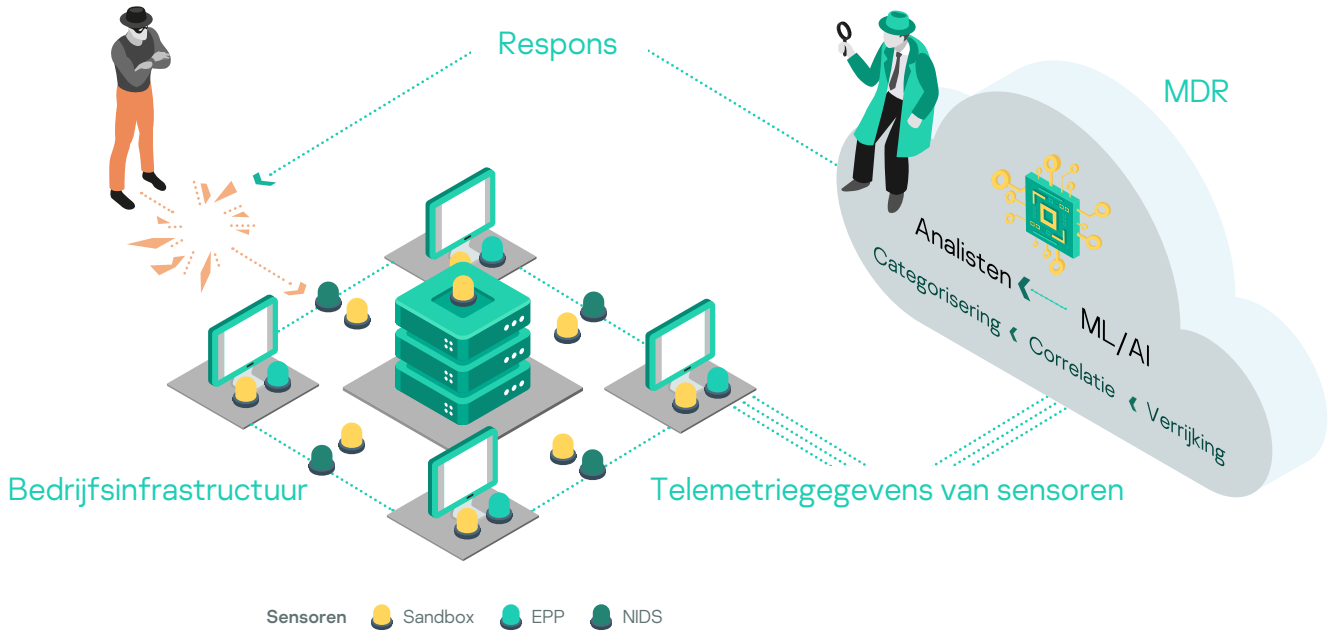
- Bij een derde van alle incidenten met grote impact ging het om doelgerichte aanvallen met menselijke tussenkomst. Geautomatiseerde tools volstaan niet om al deze aanvallen op te sporen. Het is nodig om handmatige dreigingsopsporing, in combinatie met klassieke monitoring op basis van meldingen[1], te implementeren.
- Oefeningen met professionele red teams[2] zijn erg vergelijkbaar met geavanceerde aanvallen en zijn dus een goede manier om de operationele efficiëntie van een organisatie te beoordelen.
- Bij 9% van de gerapporteerde incidenten met grote impact ging het om geslaagde pogingen tot social engineering, hetgeen het belang van beveiligingsbewustwording onder werknemers onderstreept[3].
- Wees toegerust op de detectie van alle tactieken (fasen van de attack kill chain). Zelfs complexe aanvallen bestaan uit eenvoudige stappen, ook wel 'technieken' genoemd. Detectie van een bepaalde techniek kan de hele aanval blootleggen.
- Verschillende detectietechnologieën werken efficiënt tegen verschillende aanvalstechnieken. Gebruik verschillende beveiligingstechnologieën[4] om de kans op detectie te verhogen.

[1] www.kaspersky.nl/enterprise-security/managed-detection-and-response
[2] www.kaspersky.nl/enterprise-security/security-assessment
[3] www.kaspersky.nl/enterprise-security/security-awareness
[4] www.kaspersky.nl/enterprise-security/wiki-section/products/multi-layered-approach-to-security

Inleiding

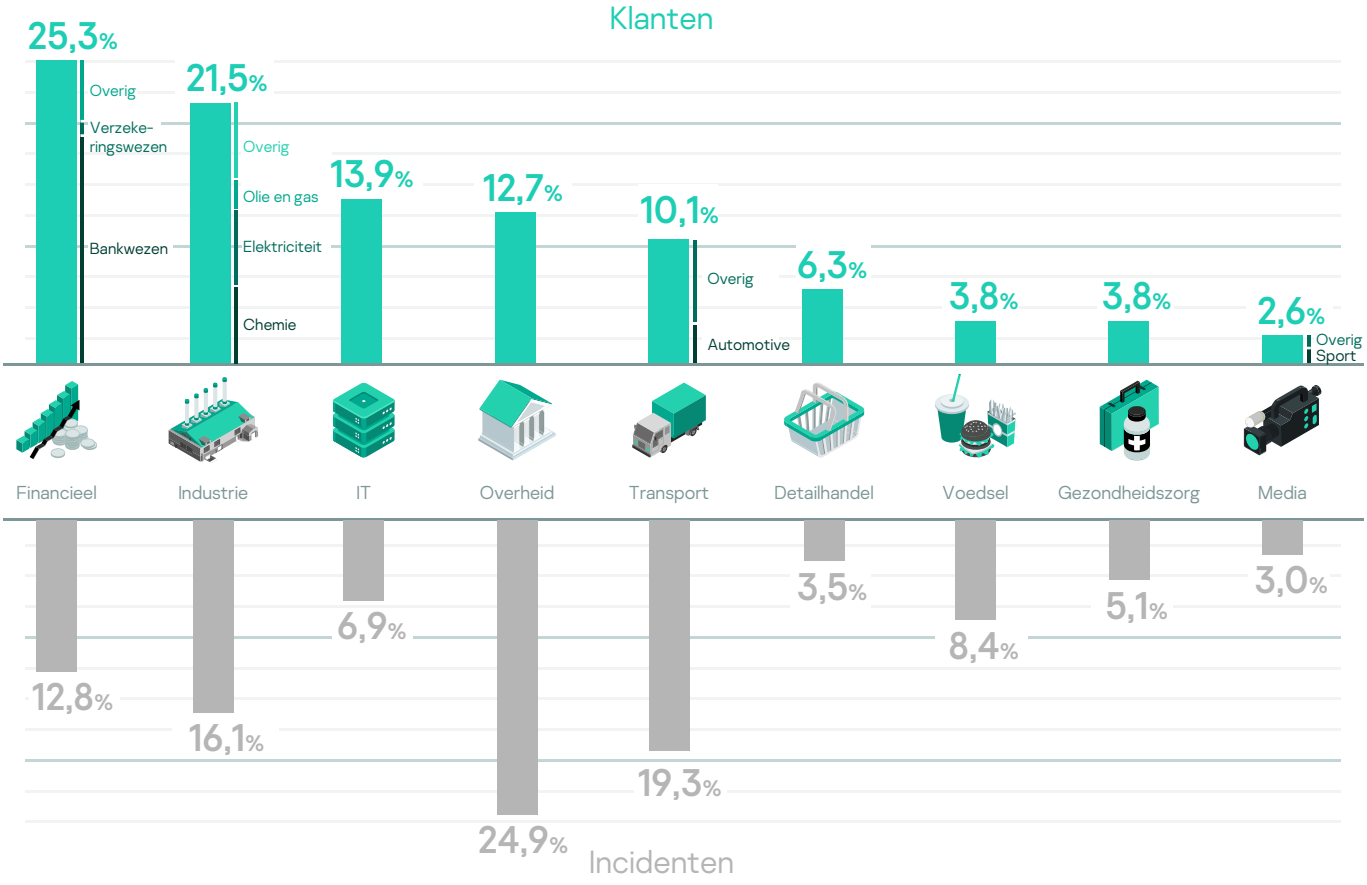
Nu cyberaanvallen steeds geavanceerder worden en beveiligingsoplossingen steeds meer resources vereisen om de enorme hoeveelheden verzamelde gegevens te verwerken, hebben veel organisaties behoefte aan hoogwaardige beveiligingsservices die deze groeiende complexiteit 24/7 en in realtime het hoofd kunnen bieden.

Volgens een schatting in de 2020 Gartner MDR Services Market Guide "gebruikt 50% van de organisaties in 2025 Managed Detection and Response-services voor dreigingsmonitoring, -detectie en -respons, om zo dreigingen te beheersen."



Dekking van MDR-service: sectoren en verticals

Zoals hieronder te zien is, wordt onze MDR-service in alle sectorverticals gebruikt. Ook ziet u het aantal gedetecteerde incidenten. Alle gegevens in het rapport betreffen Q4 2020[1].



[1]Het rapport is gebaseerd op geanonimiseerde metadata die klanten vrijwillig hebben aangeleverd sinds Q4 2020, toen de service beschikbaar was in bepaalde markten. De service is wereldwijd gelanceerd in Q1 2021

Dagelijkse MDR-routine

Een MDR-service ontvangt enorme hoeveelheden onbewerkte telemetriegegevens van sensoren, filtert en verrijkt de gebeurtenissen, zet ze om in meldingen voor dreigingsopsporing, en transformeert die tot incidenten die sneller door mensen kunnen worden aangepakt en die ook nuttig zijn voor andere beveiligingstoepassingen.

Dagelijkse gebeurtenissen van één host

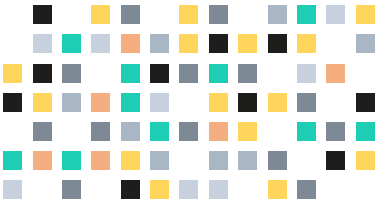
~15K

Deze waarde kan aanzienlijk schommelen, afhankelijk van de hostactiviteit

Op basis hiervan zijn

65K meldingen verwerkt

gedurende 3 maanden, afkomstig van alle sensoren

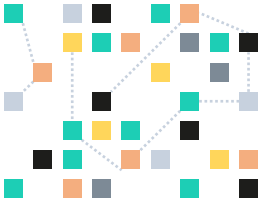


43K incidenten zijn handmatig gecategoriseerd en 22K incidenten met AI/ML

Dit leidde tot

1506 incidenten

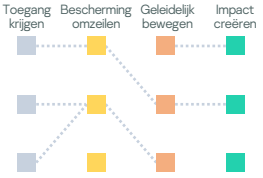
die aan klanten werden gerapporteerd



- Meldingen gerelateerd aan gerapporteerde incidenten: 2566
- 5,9% van de meldingen werd in incidenten omgezet, wat betekent dat het in 94,1% van de gevallen om false positives ging

92,9%

verrijkt met ATT&CK



- 1400 incidenten kunnen worden toegewezen aan MITRE ATT&CK
- Bij andere incidenten betreft het mogelijk zichtbaarheidsincidenten of incidenten met weinig impact, waarbij het niet nodig is om het framework te gebruiken

Effectiviteit van incidentneutralisatie

Hoeveel meldingen waren er nodig om een incident te neutraliseren?

1 melding

voor 80,1% van de incidenten

Dit wijst op de algehele effectiviteit van incidentdetectie en -neutralisatie

2-4 meldingen

voor 15,3% van de incidenten

Dit geeft aan op welke punten het proces voor incidentdetectie en -neutralisatie mogelijk moet worden aangepast. In al deze gevallen wordt nieuwe detectielogica opgesteld, waarna ze worden overgezet naar de statistieken voor detectie met één melding

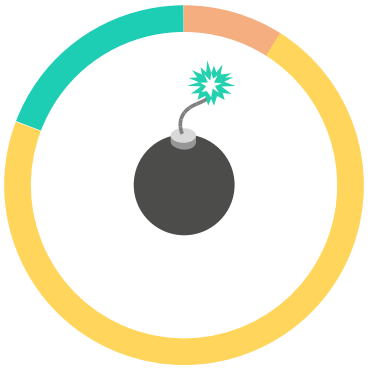
5 of meer meldingen

voor 4,6% van de incidenten

Incidenten die met veel meldingen samenhangen, betreffen gevallen waarin snelle neutralisatie niet toegestaan of niet efficiënt is:

- Nieuwe doelgerichte aanval/APT ontdekt
- Door klant aangevraagde aanvalsmonitoring zonder respons
- Beveiligingsbeoordelingen die geen respons vereisen (bijv. penetratietests)

impact van incidenten



9% **incidenten met grote impact**

Veroorzaken grote ontregeling of leiden tot ongeoorloofde toegang tot de klantassets die onder MDR vallen.

Er zijn sporen geïdentificeerd van een doelgerichte aanval of onbekende dreiging en er is aanvullend onderzoek nodig op basis van digitale forensische analyse

72% **incidenten met middelmatige impact**

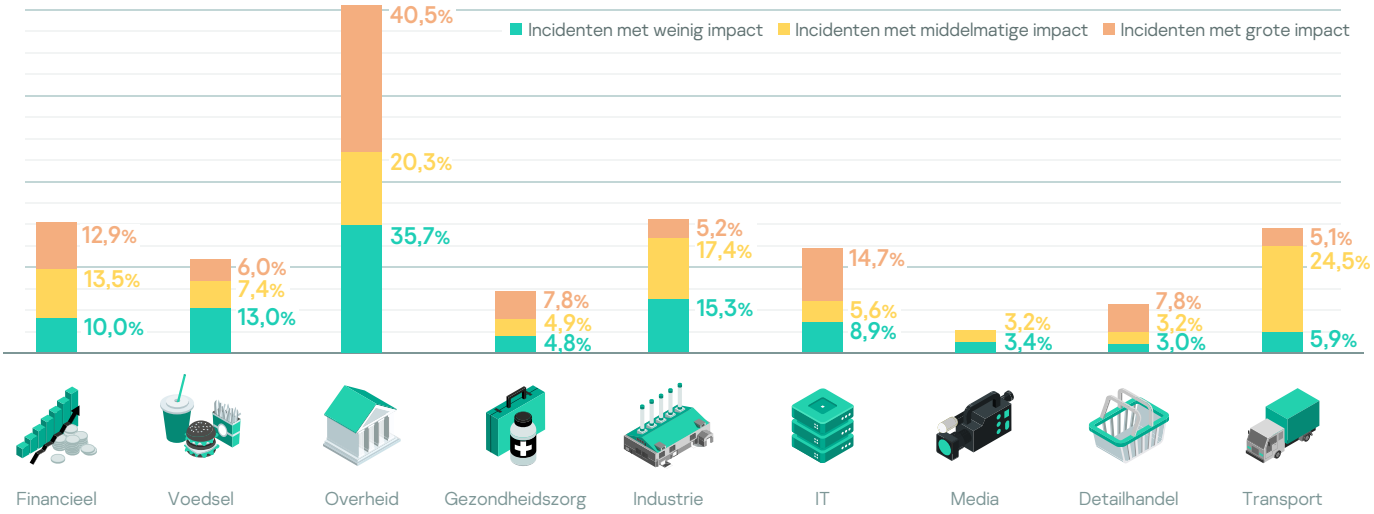
Hebben impact op de efficiëntie of prestaties van de klantassets die onder MDR vallen of leiden tot geïsoleerde gevallen van gegevenscorruptie.

19% **incidenten met weinig impact**

Hebben geen aanzienlijke impact op de efficiëntie of prestaties van de klantassets die onder MDR vallen en leiden waarschijnlijk niet tot gegevenscorruptie.

Er is ongewenste software geïdentificeerd: adware, riskware, not-a-virus enz.

Elke dag identificeerden we 1-2 grote incidenten. Alleen klanten uit de sectoren media en transport kregen in Q4 2020 niet te maken met incidenten met grote impact. De sectoren overheid, financieel en IT zagen zich voor de grootste uitdagingen gesteld in dit kwartaal.



Hoelang duurt het om een incident te identificeren?

Een melding over een verdachte gebeurtenis belandt eerst in de wachtrij en wordt dan gecategoriseerd door een menselijke analist (op AI of ML gebaseerde meldingen (~33%) worden binnen enkele seconden verwerkt en zijn hier niet weergegeven). Alle gecategoriseerde meldingen worden in incidentcasussen omgezet en door een analist onderzocht. Daarna wordt er een incidentkaart gemaakt en naar de klant verzonden. We delen de volledige tijdlijn voor meldingsverwerking (inclusief de tijd in de wachtrij) tot aan het incidentrapport.

52,6 min **grote impact**

De gevoeligste incidenten vragen om extra tijd voor verrijking en opsporing

21,1 min **weinig impact**

Incidenten met deze impact komen het vaakst voor. De kortste tijd wijst op de efficiëntie van templates voor de meestvoorkomende incidentkaarten

30,2 min **middel-matige impact**

De laagste prioriteit van deze incidenten betekent dat ze veel tijd in de wachtrij doorbrengen zodat een analist ze kan verwerken

De aard van incidenten met grote impact

Wat zijn de oorzaken van incidenten met grote impact?

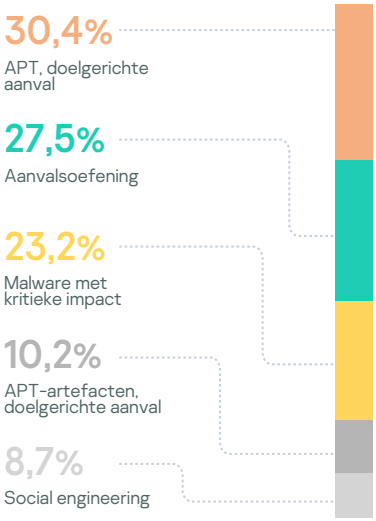
Een derde (30,4%) van alle incidenten met grote impact betrof doelgerichte aanvallen of APT's

1 op de 4 incidenten met grote impact betrof een aanvalspoging met menselijke tussenkomst (penetratietest, red teaming, aanvalssimulatie enz.)

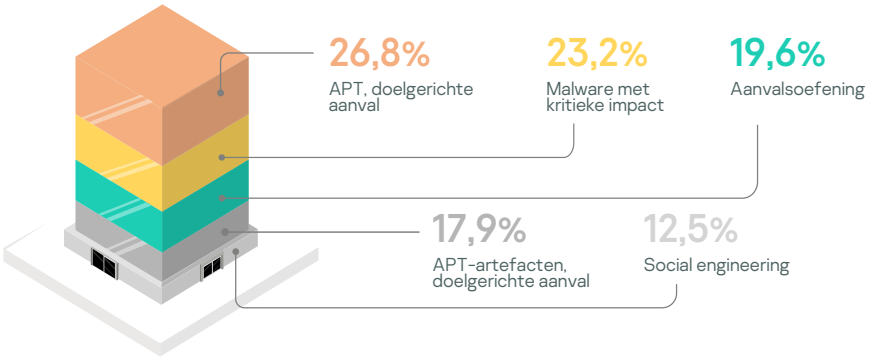
1 op de 5 incidenten betrof malware zoals ransomware (bijv. WannaCry) met een aanzienlijke impact maar zonder menselijke tussenkomst

10% betrof niet-gecategoriseerde incidenten met duidelijke tekenen van een eerdere aanval of aanvalsoefening
(zoals een Lsass-dump, kirbi-bestanden en tekenen van persistent OS). Dit gebeurde vooral bij nieuwe clients of de toevoeging van een nieuwe host aan het monitoringsysteem

Bij 9% van de incidenten werd toegang verkregen via social engineering, maar werden aanvallen voorkomen voordat ze konden worden gecategoriseerd



Hoeveel organisaties hadden te maken met incidenten met grote impact?



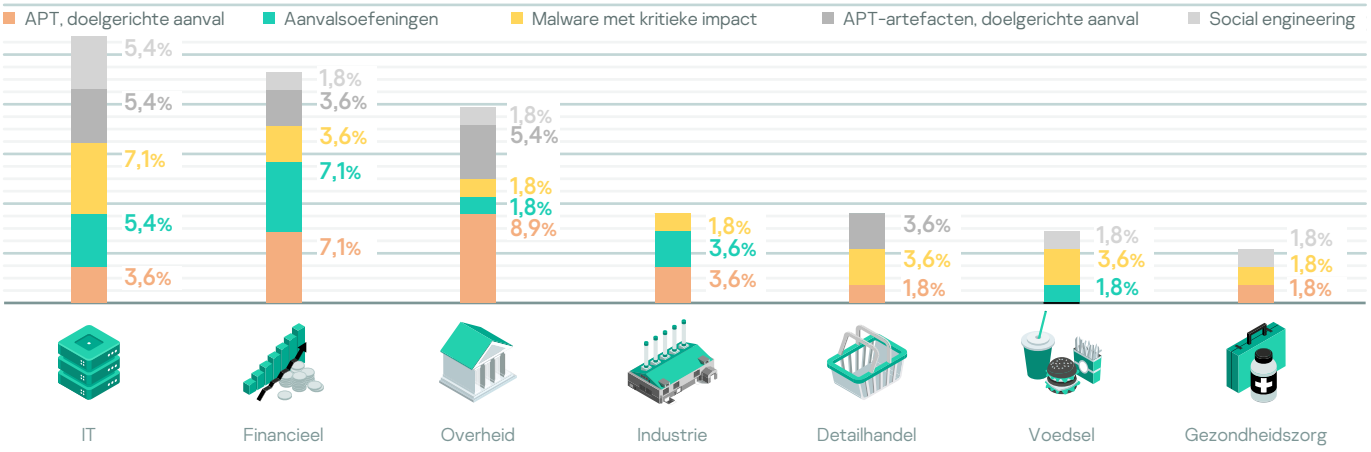
27% van de organisaties kreeg te maken met een doelgerichte aanval of APT

23% werd het slachtoffer van malware met een grote impact (zoals ransomware)

20% van onze klanten deed aan aanvalsoefeningen

Aantal organisaties met ernstige incidenten, per vertical

Bijna alle sectoren hadden te maken met alle soorten incidenten gedurende onze analyseperiode van drie maanden.



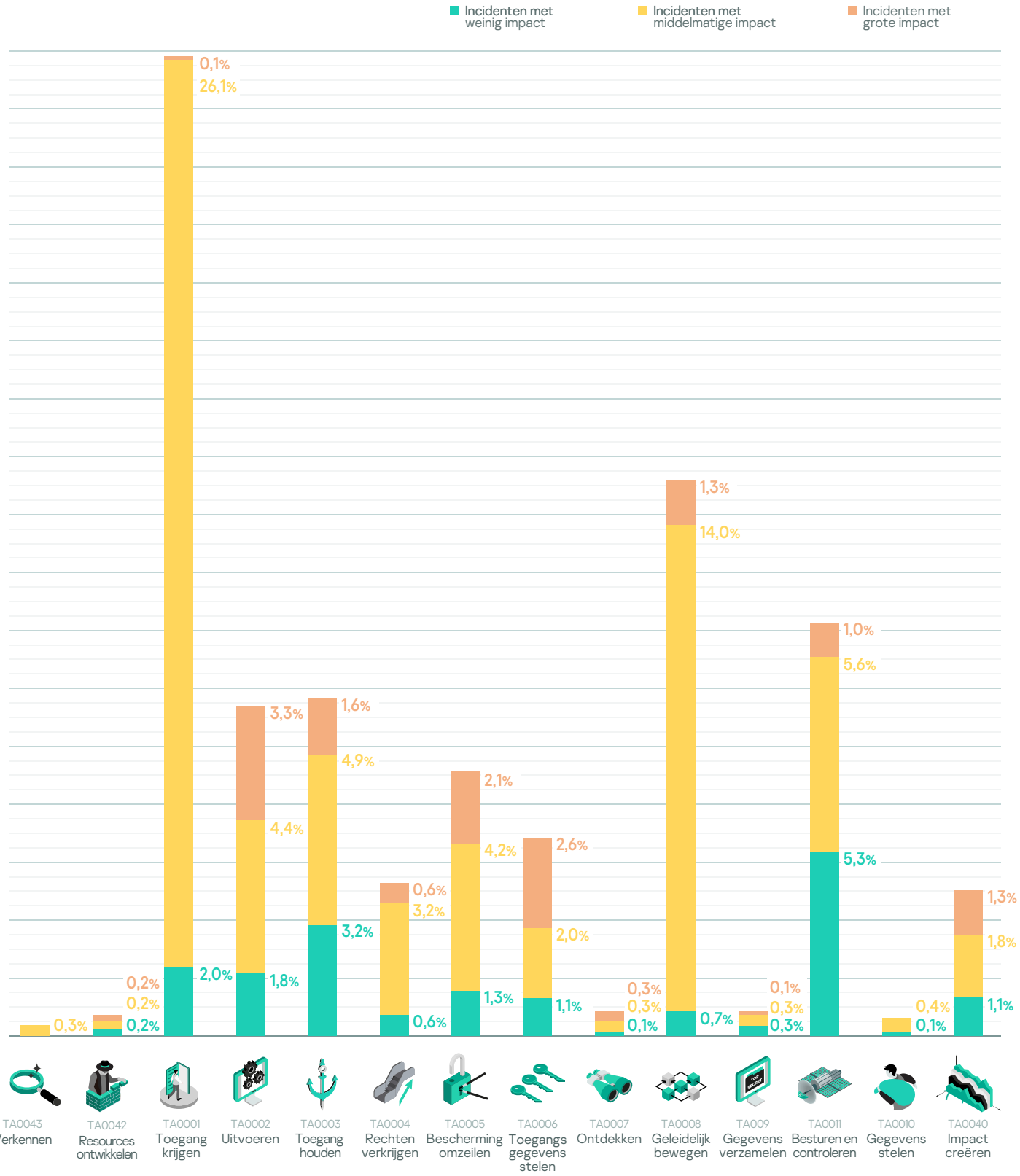
Bij actieve APT's worden vrijwel altijd ook APT-artefacten (tekenen van eerdere aanvallen door mensen) aangetroffen. Dit bewijst dat organisaties die een APT hebben geneutraliseerd, vaak opnieuw worden aangevallen – waarschijnlijk door dezelfde partij.

In sectoren die het doelwit zijn van APT's, worden vaak ook red teams gevormd, wat aangeeft dat organisaties zich bewust zijn van de risico's.

Detectietechnologie en aanvals-TTP's

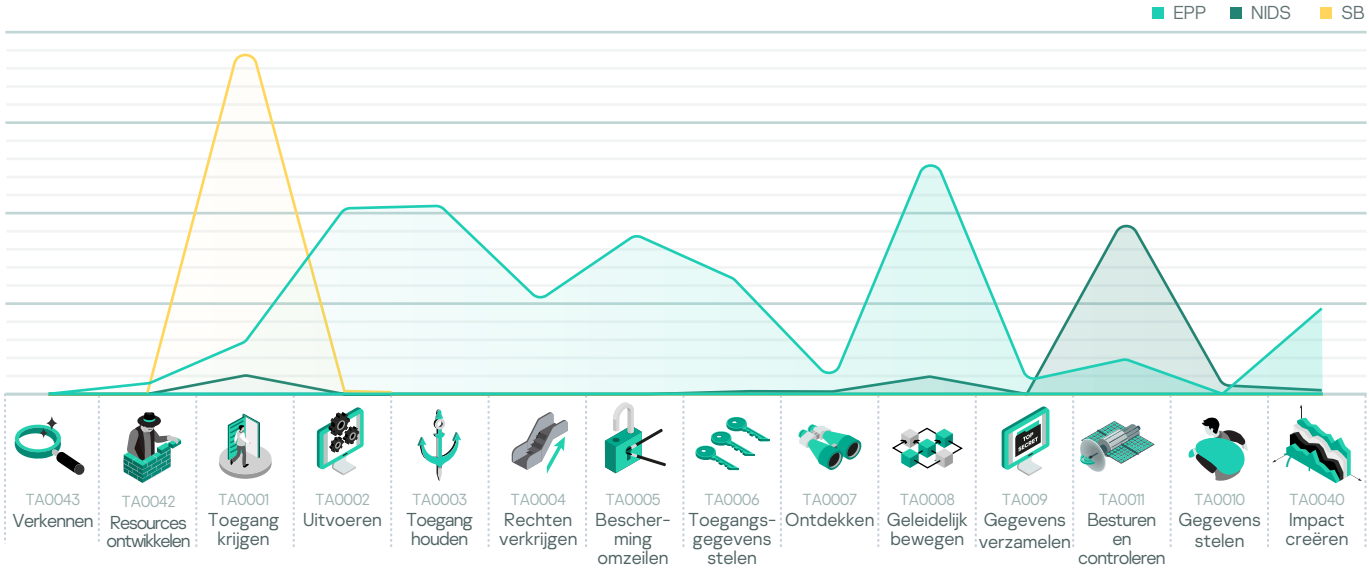
Aanvalstactieken

De meeste incidenten werden gedetecteerd in de fase 'Toegang krijgen'. Aanvalstactieken in de fasen 'Uitvoeren', 'Toegang houden', 'Bescherming omzeilen', 'Toegangsgegevens stelen', 'Geleidelijk bewegen' en 'Besturen en controleren' werden ook vaak gedetecteerd. Er werden minder incidenten gedetecteerd in de fasen 'Gegevens stelen' en 'Gegevens verzamelen' omdat aanvallen in eerdere stadia al correct waren geclassificeerd en geneutraliseerd. Alle gevallen die in deze late stadia worden gedetecteerd, worden uitgebreid geanalyseerd. Ook wordt er gekeken hoe de detectielogica kan worden verbeterd. Zo stijgt de kans dat dreigingen zo vroeg mogelijk worden gedetecteerd.



Tactieken en detectietechnologie

Bij MDR ontvangen we telemetriegegevens van verschillende soorten sensoren (detectietechnologieën): Endpoint Protection Platform (EPP), Sandbox (SB) en Network Intrusion Detection System (NIDS). Network IDS en SB zijn componenten van Kaspersky Anti-Targeted Attack Platform[1]. Hostgebaseerd NIDS maakt deel uit van het uitgebreide EPP Kaspersky Endpoint Security for Business[2]. Hieronder ziet u welke MITRE ATT&CK-technieken per sensor het vaakst worden opgepikt bij onze MDR. De grafiek laat zien welke aanvalstactiek op welk moment wordt gedetecteerd.



Hieronder ziet u welke MITRE ATT&CK-technieken per sensor het vaakst worden opgepikt bij onze MDR (op basis van het aantal incidenten)

Toegang krijgen

- EPP SB — T1566.001 Spearphishing-bijlage
- SB NIDS — T1566.002 Spearphishing-link
- NIDS — T1190 Misbruik van publieksgerichte apps
- NIDS — T1133 Externe remote services

Uitvoeren

- EPP SB — T1053 Geplande taak/opdracht
- EPP SB — T1204 Uitvoering door gebruiker
- EPP — T1059.001 PowerShell
- EPP — T1059 Vertaler voor opdrachten en scripts
- SB — T1204.001 Schadelijke link

Toegang houden

- EPP SB — T1053 Geplande taak/opdracht
- EPP — T1547.001 Uitvoersleutels in register/opstartmap
- EPP — T1546.008 Toegankelijkheidsfuncties
- NIDS — T1133 Externe remote services

Rechten verkrijgen

- EPP SB — T1053 Geplande taak/opdracht
- EPP — T1547.001 Uitvoersleutels in register/opstartmap
- EPP — T1546.008 Toegankelijkheidsfuncties
- EPP — T1055 Procesinjectie

Bescherming omzeilen

- EPP — T1036 Vermomming
- EPP — T1055 Procesinjectie

Toegangsgegevens stelen

- EPP — T1003 OS-toegangsgegevens dumpen

Ontdekken

- NIDS — T1083 Bestanden en mappen ontdekken

Geleidelijk bewegen

- EPP NIDS — T1210 Misbruik van remote services
- EPP — T1021 Remote services

Besturen en controleren

- NIDS — T1071 Toepassingslaagprotocol
- NIDS — T1095 Niet-toepassingslaagprotocol
- NIDS — T1102 Webservice

Gegevens stelen

- NIDS — T1048 Gegevens stelen via alternatief protocol

Impact creëren

- EPP — T1496 Resources kapen

EPP

- Duidelijk de grootste dekking bij alle tactieken
- Gericht op de drukste aanvalsfasen: tussen het krijgen van toegang en de gemaakte inbreuk die tot impact leidt

Sandbox

- Draagt bij aan snellere categorisering en biedt analisten extra context
- Resultaten gericht op de proloog en epiloog van de kill chain

NIDS

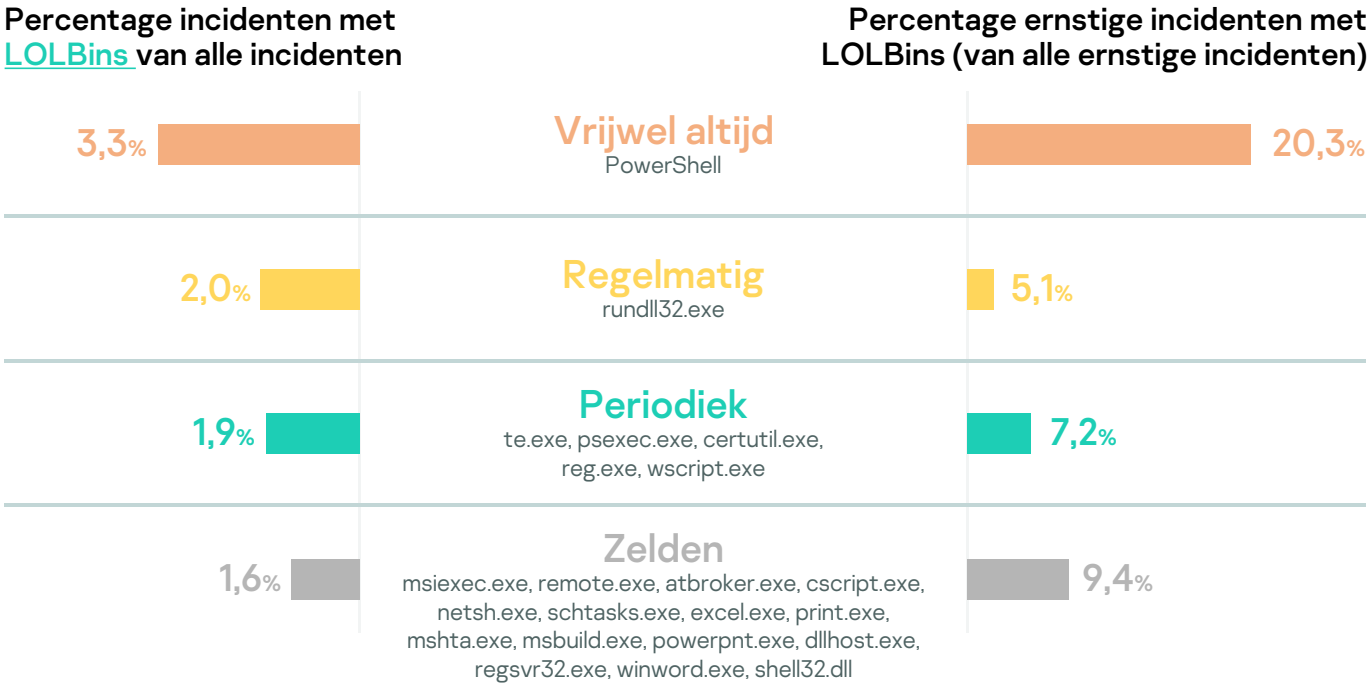
- Uitgesproken focus op tactieken die worden gebruikt voordat er impact ontstaat
- Nuttige extra bescherming tegen tactieken voor het krijgen van toegang

[1] KATA – www.kaspersky.nl/enterprise-security/anti-targeted-attack-platform
[2] KESB – www.kaspersky.nl/enterprise-security/endpoint

Aanvalstechnieken

Gebruikte tools bij incidenten

Kwaadwillenden gebruiken vaak in het OS geïntegreerde tools om instrumenten onopvallender te implementeren, om te besparen op de ontwikkeling van toolsets en bovenal om hun werk te vermengen met legitieme activiteiten, waardoor bescherming veel ingewikkelder wordt. Zulke tools worden living-off-the-land-binary's genoemd en zijn te bekijken op de website van het LOLBins-project. De hoofdconclusie is niet verrassend: hoewel Microsoft veel werk heeft verzet om de beveiliging en het beheer van PowerShell te verbeteren, blijft dit verreweg het populairste doelwit van aanvallers.



Incidenttoewijzing in MITRE ATT&CK

Efficiëntie is een nuttige statistiek voor detectielogica op basis van MITRE-technieken. Dit cijfer geeft aan welk percentage van alle gerapporteerde incidenten werd gedetecteerd door dreigingsopsporingsregels gebaseerd op bepaalde technieken.

33%

T1566: Phishing

Toont aan dat MDR effectief is tegen deze techniek vanaf de fase 'Toegang krijgen', en dat deze techniek populair is onder aanvallers

16,5%

T1210: Misbruik van remote services

Dit hangt samen met pogingen tot misbruik op afstand (zoals een groot deel van 'EternalBlue')

10,6%

T1071: Toepassingslaagprotocol

De meestgebruikte protocollen voor communicatie met infrastructuur voor besturing en controle. Ter vergelijking: T1095: 'Niet-toepassingslaagprotocol' kwam bij slechts 3,79% van de incidenten voor

5,3%

T1021: Remote services

Wordt veel gebruikt door aanvallers voor geleidelijk bewegen (T1021.002: SMB-/Windows-adminshares en T1021.001: Remote Desktop Protocol)

4,4%

T1036: Vermomming

Hierbij wordt vaak gebruikgemaakt van backdoors in toegankelijkheidsfuncties, waarbij tools zoals sethc.exe, narrator.exe, magnify.exe en ultiman.exe worden vervangen door cmd.exe. Volgens de statistieken gaat het heel zelden om incidenten met grote impact. Minder gevallen hangen samen met het hernoemen van schadelijke bestanden zodat deze er als systeemtools uitzien, of het aanmaken van geplande taken die legitiem ogen. Hierbij gaat het doorgaans om incidenten met grote of middelmatige impact

3,3%

T1204: Uitvoering door gebruiker

Hierbij betreft het succesvolle social engineering op basis van phishing-bijlagen of pogingen om van internet gedownloade software uit te voeren

6,6%

T1059: Vertaler voor opdrachten en scripts

Hierbij gaat het voornamelijk om T1059.001: PowerShell en T1059.004: Unix Shell

>0% >5% >10% >20%

TA0043: Verkennen	TA0042: Resources ontwikkelen	TA0001: Toegang krijgen	TA0002: Uitvoeren	TA0003: Toegang houden	TA0004: Rechten verkrijgen	TA0005: Bescherming omzeilen
T1595: Actief scannen	T1587: Capaciteiten ontwikkelen	T1190: Misbruik van publieksgerichte apps	T1059: Vertaler voor opdrachten en scripts	T1098: Accounts manipuleren	T1548: Misbruik van mechanisme voor hogere rechten	T1140: Bestanden of informatie ontsluieren/decoderen
	T1588: Capaciteiten verwerven	T1133: Externe remote services	T1203: Misbruik voor client-uitvoering	T1547: Automatische uitvoering tijdens opstarten of inloggen	T1134: Toegangstokens manipuleren	T1564: Artefacten verbergen
		T1566: Phishing	T1559: Communicatie tussen processen	T1037: Initialisatiescripts voor opstarten/inloggen	T1546: Uitvoering op basis van gebeurtenissen	T1562: Bescherming verzwakken
		T1091: Replicatie via verwijderbare media	T1053: Geplande taak/opdracht	T1554: Softwarebinary's van client compromitteren	T1068: Misbruik om rechten te verkrijgen	T1070: Indicatorverwijd ering op host
		T1078: Geldige accounts	T1569: Systeemservices	T1136: Accounts maken	T1574: Uitvoeringsflow kapen	T1036: Vermomming
			T1204: Uitvoering door gebruiker	T1505: Softwarecomponent en van servers	T1055: Procesinjectie	T1112: Register wijzigen
			T1047: Windows Management Instrumentatie			T1027: Versluierde bestanden of informatie
						T1542: Vóór opstarten OS
						T1218: Proxy-uitvoering van ondertekende binary

TA0006: Toegangsgegeve ns stelen	TA0007: Ontdekken	TA0008: Geleidelijk bewegen	TA0009: Gegevens verzamelen	TA0011: Besturen en controleren	TA0010: Gegevens stelen	TA0040: Impact creëren
T1110: Brute Force	T1087: Accounts ontdekken	T1210: Misbruik van remote services	T1123: Audio vastleggen	T1071: Toepassings-laagprotocol	T1048: Gegevens stelen via alternatief protocol	T1485: Gegevens vernietigen
T1555: Toegangsge-gevens uit opslaglocaties voor wachtwoorden	T1482: Domeintrusts ontdekken	T1570: Geleidelijke overdracht van tools	T1005: Gegevens uit lokaal systeem	T1001: Gegevens versluieren		T1486: Gegevens versleutelen voor impact
T1556: Authenticatieproces wijzigen	T1083: Bestanden en mappen ontdekken	T1021: Remote services	T1056: Invoer vastleggen	T1105: Overdracht van tools naar gecompromitteerd systeem		T1565: Gegevens manipuleren
T1003: OS-toe-gangsgegevens dumpen	T1046: Netwerkservices scannen	T1550: Alternatief authenticatiemate-riaal gebruiken		T1095: Niet-toepassing slaagprotocol		T1561: Schijf wissen
T1552: Onbeveiligde toegangsgegevens	T1135: Gedeelde resources in netwerken ontdekken			T1090: Proxy		T1496: Resources kapen
	T1069: Rechtengroepen ontdekken			T1219: Software voor externe toegang		
	T1012: Query-register			T1102: Webservice		
	T1018: Remote systemen ontdekken					
	T1033: Systeemei-genaar/gebruiker ontdekken					
	T1497: Virtualisaties/sandbox es omzeilen					