Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Indicators of Compromise

Pas dreigingsinformatie effectief toe

Factsheet FS-2016-02 | versie 1.0 | 8 december 2016

Als u verantwoordelijk bent voor het veilig houden van het netwerk van uw organisatie, zult u de term vaak horen: een IoC, oftewel een Indicator of Compromise. Kortweg is een IoC een aanwijzing die het mogelijk maakt de aanwezigheid van een specifieke dreiging binnen uw netwerk op te sporen.

Bij het ontvangen van een IoC vragen veel organisaties zich af wat zij met een dergelijke IoC moeten doen. Hoe moet ik een IoC verwerken? Wat ga ik dan vinden? En wat moet ik doen als ik er achter kom dat ook mijn organisatie is geraakt? Dit zijn allemaal begrijpelijke vragen waar deze factsheet antwoord op biedt.

Achtergrond

Incidenten binnen een netwerk blijven vaak lange tijd onopgemerkt. Diverse malwarecampagnes zoals *Carbanak*[1] en *SYNful Knock*[2] illustreren dat aanvallen soms jarenlang onzichtbaar kunnen blijven. Al die tijd kunnen aanvallers gevoelige informatie uit netwerken van getroffen organisaties exfiltreren zonder dat de getroffen organisaties daar zelf erg in hebben.

Doelgroep

Informatiebeveiligers

Samenwerkingspartners

Belastingdienst
ING Bank NV

[1] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
[2] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

Met behulp van Indicators of Compromise maakt u inzicht over uw eigen incidenten deelbaar met andere organisaties. De laatste jaren hebben organisaties ondervonden dat het detecteren van een digitale compromittering moeilijk is. Een incident bij een organisatie kan slechts een van meerdere soortgelijke incidenten zijn bij verschillende organisaties. Informatie over een incident binnen een organisatie kan leiden tot detectie en wellicht preventie hiervan binnen andere organisaties.

Indicators of Compromise

Een Indicator of Compromise (IoC) is informatie die kan helpen bij het identificeren van specifiek malafide gedrag op een systeem of binnen een netwerk .[3]

In de praktijk zijn IoC's vaak IP-adressen of domeinnamen. Als deze IP-adressen of domeinnamen voorkomen binnen een netwerk, kan dit duiden op een besmetting. Bijvoorbeeld, een organisatie stelt vast slachtoffer te zijn van een aanval waarbij de daders gevoelige documenten naar een externe server hebben geüpload. Om andere organisaties te helpen om een soortgelijke aanval te detecteren deelt de organisatie de tot dan toe bekende eigenschappen (IoC's) van de aanval, zoals bijvoorbeeld het IP-adres en de domeinnaam van de server. Op basis van deze informatie kunnen andere organisaties onderzoeken of binnen hun netwerk sprake is van vergelijkbare malafide activiteiten. Is dit het geval, dan is dit een indicatie dat deze andere organisaties mogelijk te maken hebben met dezelfde aanval.

Tijdens een onderzoek kunnen er meerdere aan elkaar gerelateerde IoC's beschikbaar komen rondom een incident. Met deze IoC's kunnen organisaties de kenmerken verder uitbreiden zodat zij een steeds beter beeld krijgen van het incident. Zo kan het zijn dat na verloop van tijd bekend wordt dat de aanval startte met een e-mail met een specifiek onderwerp, misbruik werd gemaakt van een bekende kwetsbaarheid, specifieke bestanden werden gebruikt en bij de communicatie met de externe server steeds eenzelfde patroon terugkeerde. Op basis hiervan kan de set IoC's voor de aanval er op een gegeven moment als volgt uitzien:

```
IP-adres: 192.168.23.29
Domein: cc.evilserver.domain
E-mailonderwerp: "Something interesting!"
Kwetsbaarheid: CVE-4242-4242
MD5-hash bestand:
24b6dc71b26debdfb8c7cfbd3a55abbd
URL-patroon: abc\d\d\d(.*?)\.php
```

[3] Er zijn standaarden waarin de definitie van een IoC afwijkt of waar dit een andere naam heeft.

Met IoC's hebben organisaties meer mogelijkheden tot het detecteren van soortgelijke aanvallen.

Het belang van contextinformatie

Het is van belang om IoC's zoveel als mogelijk te voorzien van contextinformatie. De volgende vragen kunnen helpen bij het vergaren van relevante contextinformatie:

- **Wie** is er geraakt door deze aanval? Richt de aanval zich op een specifieke organisatie, een specifieke sector of zijn meerdere organisaties en/of sectoren geraakt?
- **Wie** zit er achter deze aanval en wat is het niveau van de aanvaller? Gaat het bijvoorbeeld om een scriptkiddie of is de aanval uitgevoerd door een statelijke actor?
- **Wat** is er gebeurd en **wat** is de schade? Is een systeem tijdelijk onbereikbaar gemaakt (Denial-of-Service) of zijn er grote hoeveelheden gevoelige documenten buitgemaakt?
- **Waar** in het netwerk heeft de aanval plaatsgevonden? Richtte de aanval zich bijvoorbeeld op de werkstations binnen de organisatie of trof de aanval ICS/SCADA-systemen?
- **Wanneer** vond de aanval plaats? Dit vereenvoudigt het zoeken in de logging en bepaalt bijvoorbeeld ook of er echt een probleem is. De domeinnaam van een bonafide website die gedurende vijf minuten malware verspreidde kan een geldige IoC zijn, maar enkel hits binnen deze vijf minuten zijn dan relevant.
- **Waarom** is deze aanval uitgevoerd? De waarom-vraag kan helpen om te bepalen hoe groot de kans is dat een andere organisatie ook wordt geraakt.

Lever altijd zo veel mogelijk contextinformatie bij een IoC. Dit zal in de praktijk vaak beperkt zijn. Soms zijn organisaties bewust terughoudend bij het delen van informatie, omdat ze bijvoorbeeld niet kenbaar willen maken dat zij slachtoffer zijn of bepaalde details rondom een aanval niet bekend willen maken.

Vertrouwelijkheid van informatie

Organisaties die elkaar vertrouwen wisselen gemakkelijker informatie met elkaar uit. Wanneer een organisatie informatie deelt en niet wil dat deze informatie verder wordt verspreid, dan moet deze organisatie kunnen vertrouwen op de manier waarop de ontvangende organisaties met deze informatie omgaan.

Met het Traffic Light Protocol (TLP) geeft de verstrekker van de informatie aan aan wie deze verder verspreid mag worden. Wanneer u informatie ontvangt met een TLP-aanduiding weet u wat u wel en niet met deze informatie mag doen. De term Traffic Light verwijst naar de diverse kleuren van een verkeerslicht. Een organisatie kan informatie delen onder TLP Red (rood), TLP Amber (oranje), TLP Green (groen) of TLP White

(wit). Onderstaande tabel geeft een kort overzicht van de TLP-categorieën.

TLP-categorieën

TLP-RED	"For your eyes only". Alleen door u te gebruiken en niet voor verspreiding naar andere personen, zelfs niet binnen uw organisatie.
TLP-AMBER	Te gebruiken en te delen met collega's binnen uw organisatie op basis van need-to-know en met klanten die deze informatie moeten krijgen zodat zij zichzelf kunnen beschermen of verdere schade hiermee kunnen voorkomen.[4]
TLP-GREEN	Niet al te gevoelige informatie die u mag verspreiden naar al uw contacten zolang u het niet publiceert op een openbare plek zoals een blog of website.
TLP-WHITE	Openbare informatie die vrij verspreid mag worden, rekening houdend met het auteursrecht.

Bepaal bij het beschikbaar stellen van uw eigen IoC's in hoeverre u verdere verspreiding ervan toestaat en kies de juiste TLP-categorie. Bedenk daarbij dat het classificeren van informatie als TLP Red dusdanige beperkingen oplegt dat het de vraag is of het nog wel nuttig is deze informatie te delen. Houd bij het verwerken van IoC's die u van anderen ontvangt ook rekening met de TLP-categorie die de melder heeft meegestuurd.

Indien u het beheer van (een deel van) uw infrastructuur heeft uitbesteed aan een derde partij, bedenk dan dat eventuele beperkingen met betrekking tot de TLP-categorie betekenen dat IoC's die u ontvangt niet altijd gedeeld mogen worden met deze partij. In geval van twijfel adviseren wij u navraag te doen bij de partij die de informatie met u heeft gedeeld.

Toepassing van IoC's

Om IoC's binnen uw organisatie toe te kunnen passen zult u, afhankelijk van de grootte van uw organisatie, hier een of meerdere mensen met inhoudelijke kennis voor in huis moeten hebben. Daarnaast moet u op centrale systemen binnen uw organisatie logging ingeschakeld hebben. U kunt specifieke tooling gebruiken om binnen uw organisatie te zoeken naar hits op IoC's. Hoe u dit binnen uw organisatie het beste in kunt vullen valt buiten de scope van deze factsheet [5].

Vaak zijn er binnen een organisatie systemen die kunnen helpen bij de zoektocht naar hits op IoC's. Ter inspiratie:

- **Proxyservers** registreren de websites die gebruikers bedoeld of onbedoeld bezoeken. Domeinnamen en URL's zijn terug te vinden in de logging van deze systemen.
- **DNS-servers** geven antwoord op de DNS-verzoeken die systemen binnen de organisatie doen. Logging van DNS-servers is essentieel bij het zoeken naar malafide IP-adressen, domeinnamen en DNS-servers.
- **Mailservers** worden gebruikt voor het ontvangen of verzenden van e-mailberichten. U kunt logging van mailservers gebruiken om te zien of uw organisatie specifieke malafide e-mailberichten heeft ontvangen door te zoeken op specifieke onderwerpen, bijlages of afzenders.
- **Firewalls** monitoren allerlei netwerkstromen binnen het netwerk en kunnen verkeer toelaten of blokkeren op basis van regels. Geavanceerde firewalls kijken naast IP-adressen en poorten ook naar andere zaken. De logging van firewalls kan daarom van grote waarde zijn.
- **Intrusion Detection Systems** (IDS) en **Intrusion Prevention Systems** (IPS) zijn ingericht om aanvallen op een netwerk te herkennen of tegen te houden. Het is nuttig om te kijken of een IDS of IPS een IoC al eerder heeft opgemerkt. Zo niet, dan is het verstandig om detectieregels aan deze systemen toe te voegen zodat deze IoC in het vervolg wel zal worden herkend of tegengehouden.
- **Antivirussoftware** richt zich op de afzonderlijke systemen binnen een organisatie. Zulke software heeft zicht op de bestanden en processen die op deze systemen aanwezig zijn. Door de antivirussoftware te voorzien van informatie over malafide bestanden en processen is het mogelijk de aanwezigheid van zulke bestanden en processen op te merken op de verschillende systemen binnen de organisatie.
- Een **Security Information and Event Management** (SIEM) oplossing is bij uitstek geschikt als bron omdat hij als centraal systeem loginformatie bevat die hij vanuit allerlei systemen en applicaties krijgt aangereikt.

Begin met IoC's die ingezet kunnen worden op systemen waar informatie over (delen van) het interne netwerk op voorbij komt of verzameld wordt. Denk dan bijvoorbeeld aan SIEM-oplossingen, mailservers of proxyservers. Op deze manier kan

[4] De TLP-Amber definitie is recent gewijzigd. Bij de oude definitie mocht informatie enkel binnen de eigen organisatie verspreid worden. De nieuwe definitie biedt ruimte om dit ook, wanneer nodig, met klanten te delen. Om vertrouwensbreuken te voorkomen, vraag bij twijfel de verzender van de informatie welke definitie van TLP-Amber wordt gehanteerd. Zie ook: https://www.first.org/tlp

[5] Voor meer informatie over het implementeren van detectie-oplossingen, zie onze whitepaper Handreiking voor implementatie van detectie-oplossingen: https://www.ncsc.nl/actueel/whitepapers/handreiking-voor-implementatie-van-detectie-oplossingen.html

een IoC snel ingezet worden om voor vele verschillende systemen binnen het netwerk te monitoren. Soms zijn er alleen IoC's beschikbaar om op individuele systemen te zoeken. Vaak kunt u in deze gevallen uit contextinformatie van de IoC's het type systeem afleiden waar deze IoC van toepassing is (mailserver, webserver, werkstation, etc). Dit verkleint het zoekgebied vaak aanzienlijk.

Ik zie een hit op een IoC, en nu?

Wanneer u op een of meerdere IoC's een hit ziet, zult u moeten bepalen waar u actie wilt ondernemen. Om te bepalen of een hit actie vereist, zult u dieper moeten kijken om een duidelijk beeld van de situatie te krijgen.

Bekijk de IoC waar een hit op is gevonden goed. Een hit op een IoC betekent niet altijd dat er malafide activiteit heeft plaatsgevonden. Het kan ook een false positive betreffen. Een false positive is een onterechte hit op een IoC. Het gedrag waardoor de hit ontstaat is dan niet malafide.

Sommige IoC-types zijn gevoeliger voor false positives dan andere. Een goed voorbeeld hiervan zijn IP-adressen. Soms wordt een IP-adres exclusief gebruikt voor malafide activiteiten, maar in andere gevallen betreft het een IP-adres dat gebruikt wordt voor shared webhosting. Dan kan het zijn dat een IP-adres waar meerdere websites op bereikbaar zijn slechts één malafide website herbergt. Indien u dan een hit ziet op dit IP-adres, betekent dit niet automatisch dat dit malafide activiteiten betreft. Het kan ook een verbinding zijn naar een van de bonafide websites op dit IP-adres. Daarentegen heeft een hit op een hashwaarde van een malafide bestand een zeer lage kans om een false positive te zijn. Om deze reden kan het nodig zijn aanvullende context te creëren, bijvoorbeeld door in DNS-servers te achterhalen welke domeinnaam er is opgevraagd die tot een hit op een IoC van een IP-adres leidde.

Als u een hit vindt op een IoC, achterhaal dan welk systeem binnen het netwerk deze hit precies heeft opgeleverd. Waar u zult moeten zoeken is afhankelijk van het type IoC dat een hit heeft opgeleverd. Zodra u weet welk systeem binnen het netwerk de hit heeft opgeleverd, kunt u hier actie op ondernemen door bijvoorbeeld het systeem te isoleren van het netwerk. Ook kunt u aanvullende handelingen overwegen, zoals forensisch onderzoek. De te nemen acties zullen per organisatie en per casus verschillen. Zo zal een besmetting van een systeem van een bezoeker die op het openbare wifinetwerk zit minder belangrijk zijn dan een besmetting op de interne mailserver en zullen hier waarschijnlijk ook verschillende acties genomen worden.

Hoe kan ik zelf een Indicator of Compromise opstellen?

Inventariseer eerst welke informatie u heeft over het incident.

Kies een startpunt voor de informatievergaring, zo dicht mogelijk bij de bron van infectie. Als u enkel meta-informatie heeft (onderwerp van een e-mail, een patroon in een opgevraagde URL, etc), zult u op basis van deze informatie in systemen moeten zoeken om de daadwerkelijke bron van infectie binnen uw organisatie te achterhalen.

Is de informatie die u voorhanden heeft bestandsgebaseerd, vergaar dan unieke kenmerken van deze bestanden die u als IoC kunt toepassen en verspreiden. Wanneer u malafide bestanden aantreft, kunt u dit verifiëren, bijvoorbeeld door deze bestanden te laten scannen door uw antivirussoftware. In de meeste gevallen zal deze de bestanden herkennen als malafide. Voor bestanden zijn er verschillende kenmerken die u als IoC kunt delen. Ter inspiratie:

- De **hashwaarde** van het bestand (MD5/SHA1/SHA-256). Deze hashwaarde is karakteristiek voor het bestand zodat andere partijen deze hash kunnen gebruiken om hetzelfde malafide bestand binnen hun organisatie te herkennen.
- De **locatie** en **naam** van het bestand. Vaak kopieert malware zichzelf naar een specifieke locatie op het systeem en hernoemt hij de kopie van zichzelf zodat hij zichzelf bij een herstart van het geïnfecteerde systeem weer op kan starten.
- **Kenmerkende patronen** binnen een malafide bestand. Het komt vaak voor dat er allerlei varianten van een malafide bestand worden ingezet door kwaadwillenden. Deze bestanden zijn allemaal in essentie dezelfde malware. Elk bestand verschilt op kleine punten van de andere bestanden. Dit doen aanvallers om detectie op basis van bijvoorbeeld de hashwaarde van een bestand te voorkomen. Deze bestanden delen vaak wel dezelfde patronen in de inhoud. Met specifieke tooling zoals Yara[6] kunt u regels schrijven om malafide bestanden te herkennen op basis van patronen in de inhoud.
- **Specifieke registersleutels** die door de malware worden aangemaakt of geraadpleegd. Sommige Windows-malware zal wijzigingen in het register willen doen om bijvoorbeeld beveiligingsinstellingen op geïnfecteerde systemen te wijzigen, instellingen van de malware op te slaan of in te stellen dat de malware bij elke herstart van het systeem wordt uitgevoerd. Deze registersleutels kunnen zo uniek zijn dat deze ook als valide IoC kunnen fungeren.

[6] https://plusvic.github.io/yara/

Is de informatie die u voorhanden heeft netwerkgebaseerd, vergaar dan kenmerken van het netwerkverkeer die karakteristiek zijn voor het malafide gedrag. U kunt bijvoorbeeld logbestanden van de proxyserver of DNS-server doorzoeken op sporen van verdachte activiteiten. U kunt ook de malware uitvoeren in een gecontroleerde omgeving om netwerkverkeer te monitoren. Dit kan voldoende informatie opleveren om IoC's uit op te stellen. Op netwerkniveau kunt u bijvoorbeeld denken aan:

- **Domeinnamen**, **IP-adressen** of **URL's** waar de malware verbinding mee maakt of waar de malware van wordt gedownload.
- De **User Agent http-header** wordt door sommige malware gebruikt bij het maken van http-verzoeken. Dit doen aanvallers om zich voor te doen als een browser om minder op te vallen tussen het legitieme netwerkverkeer binnen een organisatie. Deze User Agent header is soms zo specifiek dat deze afwijkt van de User Agent header die door legitieme browsers wordt gebruikt. Dit kan een goede IoC zijn om binnen de organisatie op te monitoren.
- **Kenmerkende patronen** in het netwerkverkeer. Net zoals bestanden kan ook netwerkverkeer patronen bevatten waar een goede IoC van kan worden gebouwd. Veel malwarefamilies communiceren op zo een unieke manier met de Command & Control-servers dat dit een uitstekende manier is om binnen het netwerk te monitoren op verdachte activiteiten. Hiervoor is specifieke tooling met bijbehorende regelsets nodig, zoals Snort[7], Suricata[8] of Bro[9].

Als u zelf IoC's heeft opgesteld, controleer dan of deze IoC's geen false positives opleveren. Als u bestandsnamen gebruikt als IoC's, controleer dan op niet-geïnfecteerde systemen of deze bestandsnamen ook daadwerkelijk niet aanwezig zijn. Gebruikt u domeinnamen of IP-adressen als IoC's, controleer dan de logging van uw systemen. Het is belangrijk om zeker te weten dat deze IoC's alleen resulteren in hits als er infecties zijn.

Tot slot

Het verwerken van IoC's binnen uw organisatie is een proces waar u aparte workflows en tooling voor zult moeten inrichten en tijd voor zult moeten uittrekken. Het kan een proces zijn dat u al langer toepast, of het kan een compleet nieuwe stap zijn in de informatiebeveiliging binnen uw organisatie. Het is een proces dat helpt, maar geen garantie geeft op daadwerkelijke detectie van infecties.

Wanneer uw organisatie zich dit proces voldoende eigen heeft gemaakt is het een krachtig middel om u te weren tegen verschillende dreigingen. Ook helpt het om kennis rondom dreigingen te kunnen delen met andere organisaties, waarmee u incidenten binnen andere organisaties wellicht kunt helpen voorkomen.

[7] https://www.snort.org/
[8] http://suricata-ids.org/
[9] https://www.bro.org/

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-02 | versie 1.0 | 8 december 2016