

## SUNBURST indicator detection in QRadar

Archived: 2026-04-05 15:11:51 UTC

Estimated reading time: 6 minutes

This week, and based on current information as of the time of publication, [SolarWinds announced a cyberattack](#) that inserted a vulnerability into the SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1. This vulnerability could enable an attacker to compromise the server(s) on which SolarWinds runs, and thus gain a foothold in the victim's network. Post compromise, the attacker can conduct lateral movement, data exfiltration and other threat activity.

The United States Cybersecurity and Infrastructure Security Agency (CISA) has published [Emergency Directive 21-101](#), advising Federal agencies to disconnect or power down all SolarWinds Orion products until further notice.

As with the ['FireEye Red Team Tools detection in QRadar' blog](#), in this blog we'll provide guidance that can help you use QRadar to respond quickly.

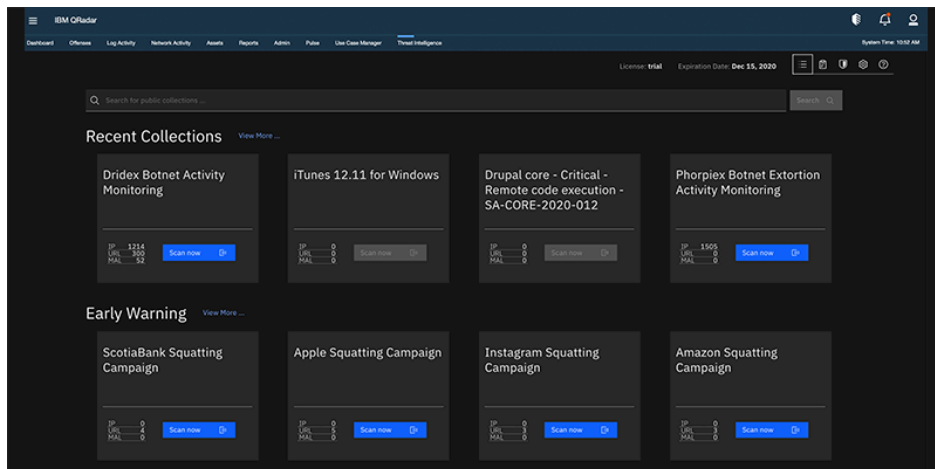
This blog will cover the following topics and content extensions:

- Threat Intelligence
  - [IBM QRadar Threat Intelligence App](#)
- Snort Rules
  - [IBM Security QRadar Custom Properties for Snort](#)
- MD5, SHA-1 and SHA-256
  - [IBM QRadar Custom Properties for Microsoft Windows](#)
  - [IBM QRadar Custom Properties for Cisco AMP](#)
  - [IBM QRadar Custom Properties for McAfee EPO](#)
  - [IBM QRadar Custom Properties for Windows Defender ATP](#)
  - [IBM QRadar Custom Properties for Carbon Black Response](#)
- Pipe creation and Sysmon
  - [IBM QRadar Custom Properties for Microsoft Windows](#)
- Endpoint content extension
  - [IBM QRadar Endpoint Content Extension](#)
  - [IBM QRadar Custom Properties for Microsoft Windows](#)
  - [IBM QRadar Custom Properties for Linux](#)
- Threat Monitoring Content Extension
  - [IBM QRadar Security Threat Monitoring Content Extension](#)

### Threat Intelligence

IBM Security X-Force researchers published a [collection of IOCs](#), including malicious file hashes, IP addresses and URLs, connected to this on-going threat. These IOCs can easily be brought into QRadar using the [Threat Intelligence App](#), which can be downloaded either from [IBM Security App Exchange](#) or natively via the [QRadar Assistant](#). Threat indicators can be added to a reference set so that they can be used within building blocks, rules and searches to detect the presence of these IOCs within your environment. Public X-Force Collections, including this one, are free to existing QRadar customers.

QRadar customers who also subscribe to the IBM Security X-Force [Advanced Threat Protection Feed](#) have access to a built-in "Am I Affected?" featured with the Threat Intelligence app. This tool can be used in tandem with other forms of threat intelligence that may become available in this developing situation to help assess known IOCs. With this subscription, new X-Force collections are loaded directly into QRadar, and users can simply click 'Scan now' to automatically search for all IOCs associated with a collection. The query results will show you which systems and users may have been connected to this threat, assisting you to initiate investigation, remediation and response.



If you do not currently subscribe to the Advanced Threat Protection Feed, a [30-day free trial](#) is available.

## Snort Rules

Once again, FireEye and Cisco Talos teams provided a new set of Snort rules to implement. QRadar users can easily create a new rule based on these signatures, correlate these insights with other events, or optionally be alerted directly via email. The steps to implement this are:

1. Install the [IBM Security QRadar Custom Properties for Snort](#) content extension
2. Create a new Event rule

Apply **Sunburst - Snort Rules** on events which are detected by the Local system and when the event(s) were detected by one or more of **Snort Open Source IDS** and when the event matches "**Rule ID**" in

(77600832,77600833,77600842,77600843,77600844,77600845,77600846,77600847,77600848,77600850,77600851,77600852,77600853,77600854,77600840,77600863,77600864,77600865,77600837,77600856,77600857,77600858,77600859,77600860,77600866,56660,56661,56662,56663,56664,56665,56666,56667,56668,56669,56670,56671,56672,56673,56674,56675,56676,56677,56678,56679,56680,56681,56682,56683,56684,56685,56686,56687,56688,56689,56690,56691,56692,56693,56694,56695,56696,56697,56698,56699,56700,56701,56702,56703,56704,56705,56706,56707,56708,56709,56710,56711,56712,56713,56714,56715,56716,56717,56718,56719,56720,56721,56722,56723,56724,56725,56726,56727,56728,56729,56730,56731,56732,56733,56734,56735,56736,56737,56738,56739,56740,56741,56742,56743,56744,56745,56746,56747,56748,56749,56750,56751,56752,56753,56754,56755,56756,56757,56758,56759,56760,56761,56762,56763,56764,56765,56766,56767,56768,56769,56770,56771,56772,56773,56774,56775,56776,56777,56778,56779,56780,56781,56782,56783,56784,56785,56786,56787,56788,56789,56790,56791,56792,56793,56794,56795,56796,56797,56798,56799,56800,56801,56802,56803,56804,56805,56806,56807,56808,56809,56810,56811,56812,56813,56814,56815,56816,56817,56818,56819,56820,56821,56822,56823,56824,56825,56826,56827,56828,56829,56830,56831,56832,56833,56834,56835,56836,56837,56838,56839,56840,56841,56842,56843,56844,56845,56846,56847,56848,56849,56850,56851,56852,56853,56854,56855,56856,56857,56858,56859,56860,56861,56862,56863,56864,56865,56866,56867,56868,56869,56870,56871,56872,56873,56874,56875,56876,56877,56878,56879,56880,56881,56882,56883,56884,56885,56886,56887,56888,56889,56890,56891,56892,56893,56894,56895,56896,56897,56898,56899,56900,56901,56902,56903,56904,56905,56906,56907,56908,56909,56910,56911,56912,56913,56914,56915,56916,56917,56918,56919,56920,56921,56922,56923,56924,56925,56926,56927,56928,56929,56930,56931,56932,56933,56934,56935,56936,56937,56938,56939,56940,56941,56942,56943,56944,56945,56946,56947,56948,56949,56950,56951,56952,56953,56954,56955,56956,56957,56958,56959,56960,56961,56962,56963,56964,56965,56966,56967,56968,56969,56970,56971,56972,56973,56974,56975,56976,56977,56978,56979,56980,56981,56982,56983,56984,56985,56986,56987,56988,56989,56990,56991,56992,56993,56994,56995,56996,56997,56998,56999,57000,57001,57002,57003,57004,57005,57006,57007,57008,57009,57010,57011,57012,57013,57014,57015,57016,57017,57018,57019,57020,57021,57022,57023,57024,57025,57026,57027,57028,57029,57030,57031,57032,57033,57034,57035,57036,57037,57038,57039,57040,57041,57042,57043,57044,57045,57046,57047,57048,57049,57050,57051,57052,57053,57054,57055,57056,57057,57058,57059,57060,57061,57062,57063,57064,57065,57066,57067,57068,57069,57070,57071,57072,57073,57074,57075,57076,57077,57078,57079,57080,57081,57082,57083,57084,57085,57086,57087,57088,57089,57090,57091,57092,57093,57094,57095,57096,57097,57098,57099,57100,57101,57102,57103,57104,57105,57106,57107,57108,57109,57110,57111,57112,57113,57114,57115,57116,57117,57118,57119,57120,57121,57122,57123,57124,57125,57126,57127,57128,57129,57130,57131,57132,57133,57134,57135,57136,57137,57138,57139,57140,57141,57142,57143,57144,57145,57146,57147,57148,57149,57150,57151,57152,57153,57154,57155,57156,57157,57158,57159,57160,57161,57162,57163,57164,57165,57166,57167,57168,57169,57170,57171,57172,57173,57174,57175,57176,57177,57178,57179,57180,57181,57182,57183,57184,57185,57186,57187,57188,57189,57190,57191,57192,57193,57194,57195,57196,57197,57198,57199,57200,57201,57202,57203,57204,57205,57206,57207,57208,57209,57210,57211,57212,57213,57214,57215,57216,57217,57218,57219,57220,57221,57222,57223,57224,57225,57226,57227,57228,57229,57230,57231,57232,57233,57234,57235,57236,57237,57238,57239,57240,57241,57242,57243,57244,57245,57246,57247,57248,57249,57250,57251,57252,57253,57254,57255,57256,57257,57258,57259,57260,57261,57262,57263,57264,57265,57266,57267,57268,57269,57270,57271,57272,57273,57274,57275,57276,57277,57278,57279,57280,57281,57282,57283,57284,57285,57286,57287,57288,57289,57290,57291,57292,57293,57294,57295,57296,57297,57298,57299,57300,57301,57302,57303,57304,57305,57306,57307,57308,57309,57310,57311,57312,57313,57314,57315,57316,57317,57318,57319,57320,57321,57322,57323,57324,57325,57326,57327,57328,57329,57330,57331,57332,57333,57334,57335,57336,57337,57338,57339,57340,57341,57342,57343,57344,57345,57346,57347,57348,57349,57350,57351,57352,57353,57354,57355,57356,57357,57358,57359,57360,57361,57362,57363,57364,57365,57366,57367,57368,57369,57370,57371,57372,57373,57374,57375,57376,57377,57378,57379,57380,57381,57382,57383,57384,57385,57386,57387,57388,57389,57390,57391,57392,57393,57394,57395,57396,57397,57398,57399,57400,57401,57402,57403,57404,57405,57406,57407,57408,57409,57410,57411,57412,57413,57414,57415,57416,57417,57418,57419,57420,57421,57422,57423,57424,57425,57426,57427,57428,57429,57430,57431,57432,57433,57434,57435,57436,57437,57438,57439,57440,57441,57442,57443,57444,57445,57446,57447,57448,57449,57450,57451,57452,57453,57454,57455,57456,57457,57458,57459,57460,57461,57462,57463,57464,57465,57466,57467,57468,57469,57470,57471,57472,57473,57474,57475,57476,57477,57478,57479,57480,57481,57482,57483,57484,57485,57486,57487,57488,57489,57490,57491,57492,57493,57494,57495,57496,57497,57498,57499,57500,57501,57502,57503,57504,57505,57506,57507,57508,57509,57510,57511,57512,57513,57514,57515,57516,57517,57518,57519,57520,57521,57522,57523,57524,57525,57526,57527,57528,57529,57530,57531,57532,57533,57534,57535,57536,57537,57538,57539,57540,57541,57542,57543,57544,57545,57546,57547,57548,57549,57550,57551,57552,57553,57554,57555,57556,57557,57558,57559,57560,57561,57562,57563,57564,57565,57566,57567,57568,57569,57570,57571,57572,57573,57574,57575,57576,57577,57578,57579,57580,57581,57582,57583,57584,57585,57586,57587,57588,57589,57590,57591,57592,57593,57594,57595,57596,57597,57598,57599,57600,57601,57602,57603,57604,57605,57606,57607,57608,57609,57610,57611,57612,57613,57614,57615,57616,57617,57618,57619,57620,57621,57622,57623,57624,57625,57626,57627,57628,57629,57630,57631,57632,57633,57634,57635,57636,57637,57638,57639,57640,57641,57642,57643,57644,57645,57646,57647,57648,57649,57650,57651,57652,57653,57654,57655,57656,57657,57658,57659,57660,57661,57662,57663,57664,57665,57666,57667,57668,57669,57670,57671,57672,57673,57674,57675,57676,57677,57678,57679,57680,57681,57682,57683,57684,57685,57686,57687,57688,57689,57690,57691,57692,57693,57694,57695,57696,57697,57698,57699,57700,57701,57702,57703,57704,57705,57706,57707,57708,57709,57710,57711,57712,57713,57714,57715,57716,57717,57718,57719,57720,57721,57722,57723,57724,57725,57726,57727,57728,57729,57730,57731,57732,57733,57734,57735,57736,57737,57738,57739,57740,57741,57742,57743,57744,57745,57746,57747,57748,57749,57750,57751,57752,57753,57754,57755,57756,57757,57758,57759,57760,57761,57762,57763,57764,57765,57766,57767,57768,57769,57770,57771,57772,57773,57774,57775,57776,57777,57778,57779,57780,57781,57782,57783,57784,57785,57786,57787,57788,57789,57790,57791,57792,57793,57794,57795,57796,57797,57798,57799,57800,57801,57802,57803,57804,57805,57806,57807,57808,57809,57810,57811,57812,57813,57814,57815,57816,57817,57818,57819,57820,57821,57822,57823,57824,57825,57826,57827,57828,57829,57830,57831,57832,57833,57834,57835,57836,57837,57838,57839,57840,57841,57842,57843,57844,57845,57846,57847,57848,57849,57850,57851,57852,57853,57854,57855,57856,57857,57858,57859,57860,57861,57862,57863,57864,57865,57866,57867,57868,57869,57870,57871,57872,57873,57874,57875,57876,57877,57878,57879,57880,57881,57882,57883,57884,57885,57886,57887,57888,57889,57890,57891,57892,57893,57894,57895,57896,57897,57898,57899,57900,57901,57902,57903,57904,57905,57906,57907,57908,57909,57910,57911,57912,57913,57914,57915,57916,57917,57918,57919,57920,57921,57922,57923,57924,57925,57926,57927,57928,57929,57930,57931,57932,57933,57934,57935,57936,57937,57938,57939,57940,57941,57942,57943,57944,57945,57946,57947,57948,57949,57950,57951,57952,57953,57954,57955,57956,57957,57958,57959,57960,57961,57962,57963,57964,57965,57966,57967,57968,57969,57970,57971,57972,57973,57974,57975,57976,57977,57978,57979,57980,57981,57982,57983,57984,57985,57986,57987,57988,57989,57990,57991,57992,57993,57994,57995,57996,57997,57998,57999,58000,58001,58002,58003,58004,58005,58006,58007,58008,58009,58010,58011,58012,58013,58014,58015,58016,58017,58018,58019,58020,58021,58022,58023,58024,58025,58026,58027,58028,58029,58030,58031,58032,58033,58034,58035,58036,58037,58038,58039,58040,58041,58042,58043,58044,58045,58046,58047,58048,58049,58050,58051,58052,58053,58054,58055,58056,58057,58058,58059,58060,58061,58062,58063,58064,58065,58066,58067,58068,58069,58070,58071,58072,58073,58074,58075,58076,58077,58078,58079,58080,58081,58082,58083,58084,58085,58086,58087,58088,58089,58090,58091,58092,58093,58094,58095,58096,58097,58098,58099,58100,58101,58102,58103,58104,58105,58106,58107,58108,58109,58110,58111,58112,58113,58114,58115,58116,58117,58118,58119,58120,58121,58122,58123,58124,58125,58126,58127,58128,58129,58130,58131,58132,58133,58134,58135,58136,58137,58138,58139,58140,58141,58142,58143,58144,58145,58146,58147,58148,58149,58150,58151,58152,58153,58154,58155,58156,58157,58158,58159,58160,58161,58162,58163,58164,58165,58166,58167,58168,58169,58170,58171,58172,58173,58174,58175,58176,58177,58178,58179,58180,58181,58182,58183,58184,58185,58186,58187,58188,58189,58190,58191,58192,58193,58194,58195,58196,58197,58198,58199,58200,58201,58202,58203,58204,58205,58206,58207,58208,58209,58210,58211,58212,58213,58214,58215,58216,58217,58218,58219,58220,58221,58222,58223,58224,58225,58226,58227,58228,58229,58230,58231,58232,58233,58234,58235,58236,58237,58238,58239,58240,58241,58242,58243,58244,58245,58246,58247,58248,58249,58250,58251,58252,58253,58254,58255,58256,58257,58258,58259,58260,58261,58262,58263,58264,58265,58266,58267,58268,58269,58270,58271,58272,58273,58274,58275,58276,58277,58278,58279,58280,58281,58282,58283,58284,58285,58286,58287,58288,58289,58290,58291,58292,58293,58294,58295,58296,58297,58298,58299,58300,58301,58302,58303,58304,58305,58306,58307,58308,58309,58310,58311,58312,58313,58314,58315,58316,58317,58318,58319,58320,58321,58322,58323,58324,58325,58326,58327,58328,58329,58330,58331,58332,58333,58334,58335,58336,58337,58338,58339,58340,58341,58342,58343,58344,58345,58346,58347,58348,58349,58350,58351,58352,58353,58354,58355,58356,58357,58358,58359,58360,58361,58362,58363,58364,58365,58366,58367,58368,58369,58370,58371,58372,58373,58374,58375,58376,58377,58378,58379,58380,58381,58382,58383,58384,58385,58386,58387,58388,58389,58390,58391,58392,58393,58394,58395,58396,58397,58398,58399,58400,58401,58402,58403,58404,58405,58406,58407,58408,58409,58410,58411,58412,58413,58414,58415,58416,58417,58418,58419,58420,58421,58422,58423,58424,58425,58426,58427,58428,58429,58430,58431,58432,58433,58434,58435,58436,58437,58438,58439,58440,58441,58442,58443,58444,58445,58446,58447,58448,58449,58450,58451,58452,58453,58454,58455,58456,58457,58458,58459,58460,58461,58462,58463,58464,58465,58466,58467,58468,58469,58470,58471,58472,58473,58474,58475,58476,58477,58478,58479,58480,58481,58482,58483,58484,58485,58486,58487,58488,58489,58490,58491,58492,58493,58494,58495,58496,58497,58498,58499,58500,58501,58502,58503,58504,58505,58506,58507,58508,58509,58510,58511,58512,58513,58514,58515,58516,58517,58518,58519,58520,58521,58522,58523,58524,58525,58526,58527,58528,58529,58530,58531,58532,58533,58534,58535,58536,58537,58538,58539,58540,58541,58542,58543,58544,58545,58546,58547,58548,58549,58550,58551,58552,58553,58554,58555,58556,58557,58558,58559,58560,58561,58562,58563,58564,58565,58566,58567,58568,58569,58570,58571,5857

**REFERENCESETCONTAINS('Sunburst - MD5', 'Parent SHA1 Hash')) OR ("SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', 'SHA256 Hash')) OR ("Parent SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', 'Parent SHA256 Hash'))**  
 AQL filter query

Enter an AQL filter query:

```
["MD5 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', 'MD5 Hash')]
OR ("Parent MD5" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', 'Parent MD5'))
OR ("SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA1', 'SHA1 Hash'))
OR ("Parent SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', 'Parent SHA1 Hash'))
OR ("SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', 'SHA256 Hash'))
OR ("Parent SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', 'Parent SHA256 Hash'))]
```

## Pipe creation and Sysmon

In the blog published by FireEye regarding SUNBURST, there is a mention about the creation of a pipe named `583da945-62af-10e8-4902-a8f205c72b2e` as one of the “delivery and installation” mechanism:

The sample only executes if the filesystem write time of the assembly is at least 12 to 14 days prior to the current time; the exact threshold is selected randomly from an interval. The sample continues to check this time threshold as it is run by a legitimate recurring background task. Once the threshold is met, the sample creates the named pipe `583da945-62af-10e8-4902-a8f205c72b2e` to act as a guard that only one instance is running before reading `SolarWinds.Orion.Core.BusinessLayer.dll.config` from disk and retrieving the XML field `appSettings`. The `appSettings` fields' keys are legitimate values that the malicious logic re-purposes as a persistent configuration. The key `ReportWatcherRetry` must be any value other than 3 for the sample to continue execution.

Source: [Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor](#)

If you are collecting Sysmon logs, you have another opportunity for a quick way to detect another IOC.

1. Download the [IBM QRadar Custom Properties for Microsoft Windows](#) content extension
2. Create a rule that detects the pipe name mentioned in the blog

Apply **Sunburst - Pipe Name** on events which are detected by the Local system and when the event(s) were detected by one or more of **Microsoft Windows Security Event Log** and when the event **QID is one of the following (5001836) PipeEvent (Pipe Created)** and when the event matches **PipeName (custom) is any of 583da945-62af-10e8-4902-a8f205c72b2e**

## Endpoint content extension

This time I will be quick with this one, but I wanted to renew my recommendation to download the latest version of the Endpoint content pack.

The pack has been built to detect lateral movement, reconnaissance tools, help to make the difference between a legitimate administration task from a suspicious one... All these behaviour have been mentioned in all the blogs you've read on the topic so far.

Below is the list of the rules (excluding building blocks) present in the Endpoint content extension

Attempt to Delete Shadow Copies	Ransomware IOCs Detected on Multiple Machines
Cobalt Strike Behaviour Detected	Ransomware: BadRabbit IOC in Events
Communication with a Potential Hostile Host	Ransomware: BadRabbit IOC in Flows
Communication with a Potential Hostile IP Address	Ransomware: Maze IOC in Events
Credential Dumping Activities Discovered	Ransomware: Maze Suspicious File Transfer
Critical File Deleted (Unix)	Ransomware: Petya / NotPetya IOC in Events
Critical File Permission Changed (Unix)	Ransomware: Petya / NotPetya IOC in Flows
Critical Security Tool Killed (Unix)	Ransomware: Petya / NotPetya Payload in Flows
Critical Security Tool Stopped	Ransomware: REvil IOC in Events
Detection of Malicious File or Process	Ransomware: WCry IOC in Events
Detection of Malicious IOC	Ransomware: WCry IOC in Flows



## Threat Monitoring Content Extension

The multi-task pack ! This pack is mentioned last in this blog because it is certainly going to need some tuning to be adapted to what you are looking for, but it is definitely a good help to know where to go.

As an example, thanks to your endpoint security software, you can increase the visibility on a threat spreading through the network. Indeed, this extension contains a series of rules alerting on security software.

Same Threat Detected on Multiple Hosts	Threats	Custom Rule	Event
Same Threat Detected on Multiple Servers	Threats	Custom Rule	Event
Same Threat Detected on Same Host	Threats	Custom Rule	Event
Same Threat Detected on Same Network Different Hosts	Threats	Custom Rule	Event
SMB Traffic Permitted From a Compromised Host	Threats	Custom Rule	Event
Successful Communication to a Malicious Website	Threats	Custom Rule	Event

### Rule

Apply Same Threat Detected on Multiple Hosts on events which are detected by the Local system and when an event matches any of the following BB:DeviceDefinition: AV/AM, BB:DeviceDefinition: IDS / IPS and NOT when an event matches any of the following BB:HostDefinition: Servers and when at least 5 events are seen with the same Threat Name (custom) and different Source Address in 5 minutes

All you have to do is to:

1. Ensure your device is listed in one of BB:DeviceDefinition: AV/AM or BB:DeviceDefinition: IDS / IPS Building blocks
2. Get the Threat Name parsed either by downloading one of our content extension, or creating your own extraction.

You can decide to duplicate the rules to focus the detection on SUNBURST specifically, and have a higher priority rule response (email, SNMP trap, vulnerability scan). Simply add a new filter to the original rule, catching the specific Threat Name reported by your product:

and when the event matches **Threat Name (custom) is any of Backdoor.Sunburst**

Please refer to your product documentation to get more information on the relevant detection name

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis	Suspicious		Ad-Aware	Trojan.SunBurst.A
AegisLab	Trojan.MSIL.SunBurst.mtc		AhnLab-V3	Backdoor.Win32.SunBurst.R337806
Alibaba	Backdoor.MSIL.SunBurst.912988be		ALYac	Trojan.MSIL.SunBurst
Antiy-AVL	Trojan(Backdoor)MSIL.Agent		Arcabit	Trojan.SunBurst.A
Avast	MSIL.SunBurst-B [Bd]		AVG	MSIL.SunBurst-B [Bd]
Avira (no cloud)	TR/SunBurst.AO		BitDefender	Trojan.SunBurst.A
CAT-QuickHeal	Backdoor.Sunburst		ClamAV	Win.Countermeasure.Sunburst.9809f52-0
Comodo	Backdoor#@31f3a9c9upfx		CrowdStrike Falcon	WinMalicious_confidence_100% (W)
Cylance	Unsafe		Cynet	Malicious (score: 85)
Cyren	W32/Trojan.BCCG-2955		DrWeb	BackDoor.Siggen.NET.14
Elastic	Malicious (high Confidence)		Emsisoft	Trojan.Win32.Sunburst (A)
eScan	Trojan.Sunburst.A		ESET-NOD32	A Variant Of MSIL/Sunburst.A
F-Secure	Trojan/W32/Sunburst.D		FireEye	Trojan.Sunburst.A

## Conclusion

The above steps can enable you to easily take advantage of the publicly available IOCs and Countermeasures to detect indicators of the SUNBURST threat within your environment. All of the QRadar apps, custom properties and content extensions mentioned above are available free of charge to all QRadar customers and can be downloaded either from the IBM Security App Exchange or natively via QRadar Assistant.

As usual, we build content for you, to save you time and effort, a content that you can use as a base and adapt to your environment and your needs. Don't hesitate to give us any feedback or ideas, tell us what you need.

If you are directly impacted and in need of expert assistance, you can contact the IBM Security X-Force Incident Response team, who is available to assist 24x7, at US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

---

Source: <https://community.ibm.com/community/user/security/blogs/gladys-koskas1/2020/12/18/sunburst-indicator-detection-in-qradar>