

SIGMA RULES



Sigma Rules Structure

Sections	Attributes	Value (Example)	Remark
Metadata	title	Installation of Malicious Service	Mandatory
	id	2cfe636e-317a-4bee-9f2c-1066d9f54d1a	
	status	stable	
	author	Blusapphire, SOC	
	date	2017/03/27	
	modified	2021/07/06	
	description	Detects known malicious service installs that only appear in cases of lateral movement, credential dumping, and other suspicious activities.	Optional
	references	- https://awakesecurity.com/blog/threat-hunting-for-paexec/ - https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf	
	tags	- attack.t1035 - attack.t1050	
Logsource	falsepositives	- Penetration testing	
	level	critical	
	logsource		Mandatory
	category		
	product	windows	
Detection	service	system	Optional
	definition		
	detection		
		selection: EventID: 7045 malsvc_paexec: ServiceFileName contains: '\PAExec' malsvc_wannacry: ServiceName: 'mssecsvc2.0' malsvc_persistence: ServiceFileName contains: 'net user'	Mandatory
	condition	selection and (malsvc_paexec or malsvc_wannacry or malsvc_persistence)	

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
Logsource	falsepositives
	level
	logsource
	category
	product
Detection	service
	definition
	detection
condition	

title

- در قوانین سیگما به نوعی توصیف کوتاهی از قوانین می گوییم که نشان می دهد که آن قانون چه کاری انجام می دهد یا به چه نوع رویداد امنیتی مرتبط است.
- وجود این فیلد اجباری است.
- عنوان باید کمتر از ۵۰ کاراکتر باشد.
- این فیلد باید با سبک تیتر (title) نوشته شده باشد.

```
"Django Framework Exceptions",
"Potential JNDI Injection Exploitation In JVM Based Application",
"Potential Local File Read Vulnerability In JVM Based Application",
"Potential OGNL Injection Exploitation In JVM Based Application",
"Process Execution Error In JVM Based Application",
"Potential XXE Exploitation Attempt In JVM Based Application",
"Potential RCE Exploitation Attempt In NodeJS",
"Python SQL Exceptions",
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
Logsource	falsepositives
	level
	logsource
	category
	product
Detection	service
	definition
detection	detection
	condition

id

- از شناسه فیلد اختیاری در مخزن سیگما برای ارائه **یک شناسه منحصر به فرد** استفاده می‌شود که **هرگز تغییر نمی‌کند**، در حالی که سایر مقادیر فیلد آن قانون می‌تواند در طول زمان تغییر کند.
- شناسه قوانین سیگما به شکل **UUID** می‌باشند.
(Universally Unique Identifier)

```
"bb0e9cec-d4da-46f5-997f-22efc59f3dca",
"e032f5bc-4563-4096-ae3b-064bab588685",
"4d0af518-828e-4a04-a751-a7d03f3046ad",
"d65f37da-a26a-48f8-8159-3dde96680ad2",
"c4e06896-e27c-4583-95ac-91ce2279345d",
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
Logsource	references
	tags
	falsepositives
	level
	logsource
Detection	category
	product
	service
	definition
	detection
Condition	
	condition

status

- این فیلد، ویژگی می باشد که **وضعیت اجرایی** یک قانون را نشان می دهد.
- فیلد وضعیت، شامل مقادیر، **پایدار آزمایشی** و **تست** می باشد.
- وجود این فیلد در قوانین سیگما **اختیاری** است.
- هر قانون جدید وضعیت **آزمایشی** را دارد.
- پس از **ماه ها** استفاده سازنده و بدون هیچ بازخورد منفی از جامعه،**وضعیت تست** را دریافت می کند.
- پس از **۱ سال** استفاده بدون **تغییرات قابل توجه** به غیر از فیلترها، ما یک قوانین را به عنوان **پایدار طبقه بندی** می کنیم.

```
"stable",  
"experimental",  
"test"
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
	definition
Detection	detection
	condition

author

- این فیلد، اطلاعات مرتبط با نویسنده یا ایجاد کننده قانون را نمایان می کند.
- وجود این فیلد در قوانین سیگما اختیاری است.
- فیلد نویسنده یک رشته است نه یک لیست
- چندین نویسنده با کاما "،" از هم جدا می شوند.
- نوع مشارکت در قانون با پرانتز مشخص می شود. مثال:

```
"Thomas Patzke",
"Moti Harmats",
"Sagie Dulce, Dekel Paz",
"Bjoern Kimminich",
"Florian Roth (Nextron Systems), Arnim Rupp",
"Florian Roth (Nextron Systems)",
"Sittikorn S, Nuttakorn T, Tim Shelton",
```

'John Galt (idea), Florian Roth (rule)

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
	definition
Detection	detection
	condition

date & modified

- این فیلد ها، اطلاعات **تاریخ ایجاد و تاریخ تغیر** هر قانون سیگما را نشان می دهد.
- وجود این فیلد در قوانین سیگما **اختیاری** است.
- این فیلدها از قالب **YYYY/MM/DD** پیروی می کنند.
- در صورتی که مقادیر **title** و **logsource** و **level** و **detection** تغییر پیدا کند فیلد **modified** نیز تغییر پیدا می کند و در غیر این صورت نیازی به تغییر این فیلد نیست.

"2017/08/05",	"2021/09/23",
"2023/02/11",	"2020/01/21",
"2017/08/12",	"2022/12/13",
"2022/01/01",	"2021/06/29",
"2017/08/06",	"2020/02/12",
"2017/11/27",	"2020/04/16",
"2018/09/09",	

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
Detection	definition
	detection
condition	

description

- این فیلد، توضیحات و شرح مفصلی درباره **ی هر قانون** ارائه می دهد.
- این فیلد توضیح می دهد که **هر قانون** برای چه **نوع رویدادها**، **تهدیدات** و **فعالیت هایی** طراحی شده است.
- بهترین توضیحات با **Detects** شروع می شود.
- فقط از عنوان انتخاب شده استفاده نمی شود. این فیلد تا جایی که ممکن است به خوبی توضیح می دهد که آن **قانون چه معنایی** دارد.
- وجود این فیلد در قوانین سیگما **اختیاری** است.

```
"Detects potential PwnKit exploitation CVE-2021-4034 in auth logs",
"Detects relevant ClamAV messages",
"Detects suspicious modification of crontab file.",
"Detects suspicious session with two users present",
"Detects exploitation attempt using public exploit code for CVE-2018-15473",
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
Logsource	references
	tags
	falsepositives
	level
Detection	logsource
	category
	product
	service
	definition
Condition	detection
	condition

references

- این فیلد، لیستی از یک یا چند پیوند صفحات وب یا اسناد می باشد.
- از این url ها جهت اطلاعات بیشتر درمورد یک قانون استفاده می شود.
- وجود این فیلد در قوانین سیگما اختیاری است.
- پیونده ها می توانند پیوندهایی مربوط به یک پست و بلاگ یا توییت، پیوندهایی به صفحه پروژه یک ابزار هک خاص، پیوند به مشاوره، پیوندهایی به بحث هایی که تهدید شناسایی شده را بهتر توضیح می دهند، باشند.

```
[  
    "https://docs.djangoproject.com/en/1.11/ref/exceptions/",  
    "https://docs.djangoproject.com/en/1.11/topics/logging/#django-security"  
],  
[  
    "https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs",  
    "https://secariolabs.com/research/analysing-and-reproducing-poc-for-log4j-2-15-0"  
],  
[  
    "https://www.wix.engineering/post/threat-and-vulnerability-hunting-with-application-server-error-logs"  
],
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
Logsource	references
	tags
	falsepositives
	level
Detection	logsource
	category
	product
	service
	definition
Condition	detection

```
[  
    "attack.initial_access",  
    "attack.t1566.001",  
    "attack.execution",  
    "attack.t1204.002",  
    "attack.command_and_control",  
    "attack.t1071.001"  
],  
[  
    "cve.2022.26134",  
    "cve.2021.26084"  
],
```

tags

- این فیلد، از تگ های CAR، MITER ATT&CK و برجسب ها برای اعداد CVE استفاده می کند.
- وجود این فیلد در قوانین سیگما اختیاری است.
- تگ ها مواردی مانند ویژگی ها یا شرایط حملات، دسته های حملات، نوع تهدیدات یا حملات، سطح وقوع حملات، منابع یا ابزار ها، دامنه های مرتبط، موضوعات مرتبط، منابع اسیب پذیری یا آلودگی و ... را بررسی می کند.
- فقط از برجسب های حروف کوچک استفاده می شود.
- در نام تگ ها از ":" و "-" استفاده می شود.
- جای خالی را با خط زیر "_" جایگزین می شوند.

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
	definition
Detection	detection
	condition

tags

- برای نشان دادن ویژگی‌های مرتبط با شناسه‌های CVE (Common Vulnerabilities and Exposures) مانند cve.*: ◦
cve.2022.41120.
- برای نشان دادن دسته‌های مختلف حملات امنیتی، مانند attack_group.*: ◦
attack_group.1 .
- برای نشان دادن انواع مختلف تهدیدها یا حملات امنیتی، مانند threat_type.*: ◦
threat_type.malware برای نوع مخرب.
- برای نشان دادن سطح پیچیدگی حملات، مانند attack_difficulty.*: ◦
attack_difficulty.medium برای حملات با سطح متوسط.
- برای نشان دادن نام ابزارها یا منابع مورد استفاده در حملات، مانند tool.*: ◦
tool.spearphishing.
- برای نشان دادن دامنه‌های مرتبط با تهدیدها یا حملات، مانند domain.*: ◦
domain.malicious.com.
- برای نشان دادن موضوعات یا دسته‌های مختلف مرتبط با قوانین، مانند theme.*: ◦
theme.ransomware.
- برای نشان دادن منابع آسیب‌پذیری یا آلودگی، مانند vulnerability.*: ◦
vulnerability.sql_injection.
- برای نشان دادن نوع زیرساخت یا سیستم‌های مرتبط، مانند infra.*: ◦
infra.web_application.

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
Logsource	references
	tags
	falsepositives
	level
Detection	logsource
	category
	product
	service
	definition
Condition	detection
	condition

false positives

- این فیلد، در مورد **شرایط مثبت کاذب احتمالی** که می تواند باعث ایجاد این قانون نیز می شود، توضیحاتی ارائه می دهد.
- وجود این فیلد در قوانین سیگما **اختیاری** است.
- این فیلد می تواند به تحلیلگر کمک کند تا چه تصمیمی برای نحوهی ادامه دادن یا پیگیری هشدار بگیرد.
- با استفاده از به **روزرسانی قانون** یا **فهرستی از موارد کاذب** شناخته شده می توان با تشخیص های نادرست مقابله کرد.

```
[  
    "Legit administrative action"  
,  
[  
    "If this was approved by System Administrator."  
,  
[  
    "Increase of users in the environment"  
,  
[  
    "Known Legacy Accounts"  
,
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
Logsource	references
	tags
	falsepositives
	level
Detection	logsource
	category
	product
	service
	definition
Condition	detection
	condition

- این فیلد، شدت و اولویت قوانین سیگما را می شخص می کند.
- وجود این فیلد در قوانین سیگما اختیاری است.
- قوانین سطح بالا و بحرانی یک حادثه را نشان می دهد (اگر مثبت کاذب نباشد)
- قوانین سطح پایین و متوسط نشان دهنده فعالیت مشکوک و نقض خط مشی است
- قوانین سطح اطلاعاتی دارای ویژگی اطلاعاتی هستند و اغلب برای اهداف انطباق یا همبستگی استفاده می شوند
- دسته بندی قوانین:
- قوانینی که خصلت آموزنده دارند (پایین، متوسط).
- قوانینی که باید یک هشدار اختصاصی را ایجاد کند (بالا، بحرانی)

level

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
	definition
Detection	detection
	condition

- هر قانون سیگما باید **منابع گزارش هایی را که تجزیه و تحلیل می کند**، مشخص کند. این فیلد، منشا و مبدأ رویداد گزارش را مشخص می کند.
- لاگسورس شامل یک یا چند فیلد از چهار فیلد زیر می شود:
Category, product, service, definition
- در حالی که این فیلد ها اختیاری هستند، یک قانون باید **حداقل یکی** از انها را شامل شود، زیرا اطلاعاتی حیاتی را در مورد تشخیص ارائه می دهد.

```
{  
    "category": "application",  
    "product": "sql",  
    "definition": "Requirements: application error logs must be collected (with LOG_LEVEL ERROR and above)"  
},  
{  
    "category": "application",  
    "product": "velocity",  
    "definition": "Requirements: application error logs must be collected (with LOG_LEVEL=ERROR and above)"  
},
```

```
logsource:  
  product: linux  
  service: auth  
---  
logsource:  
  product: cisco  
  service: aaa  
  category: accounting  
---  
logsource:  
  product: zeek  
  service: kerberos
```

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
Detection	definition
	detection
condition	

- برای انتخاب تمام گزارش‌های تولید شده توسط یک محصول خاص استفاده می‌شود، به عنوان مثال، ویندوز، اوراکل، آپاچی
- انواع محصولات می‌توانند یک گام فراتر بروند، مانند انواع Windows EventLog، به عنوان مثال، امنیت، سیستم، Windows Defender و Application 'AppLocker

```
product: windows  
category: process_creation
```

```
"sql",  
"spring",  
"rpc_firewall",  
"python",  
"qualys",  
"huawei",  
"juniper",  
"linux",
```

product

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
	definition
Detection	detection
	condition

در مثال بالا، قانون یک دسته خاص به نام process_creation برای نشان دادن اینکه این قانون از رویدادهای "Process Creation" استفاده می کند استفاده می شود.

سوال:

به چه معناست؟

Microsoft-Windows-Security-Auditing/EventID 4688 یا Sysmon/EventID 1

```
"proxy",  
"ps_module",  
"file_access",  
"pipe_created",  
"process_access",  
"firewall",  
"file_rename",  
"dns_query",
```

```
product: windows / service: security  
product: windows / category: process_creation  
product: windows / category: ps_module  
product: windows / category: ps_script
```

- سیگما فقط درمورد موارد رو به رو
- دایکیومنت تهیه کرده است.

category

- لاغ های مشخصی از گروهی از محصولات هستند.
firewall, process_creation, file_event.

Sigma rules

definition

◦ در این قسمت، اطلاعات اضافی مربوط به گزارش را وارد می کنیم که می تواند شامل نیازمندی ها باشد.

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
Logsource	tags
	falsepositives
	level
	logsource
	category
Detection	product
	service
	definition
	detection
	"Requires the 'eDiscovery search or exported' alert to be enabled", 'Requirements: cisco ldp logs need to be enabled and ingested', 'Requirements: huawei bgp logs need to be enabled and ingested', 'Requirements: enable Object Access SAM on your Domain Controllers' 'Requirements: ParentUser field needs sysmon >= 13.30', 'fields have to be extract from event',
Condition	

Sigma rules

Sections	Attributes
Metadata	title
	id
	status
	author
	date
	modified
	description
	references
	tags
	falsepositives
Logsource	level
	logsource
	category
	product
	service
Detection	definition
	detection
condition	

detection

- در این قسمت آنچه را که در لگ ها به دنبال آن هستیم تعریف می کنیم.
- این بخش شامل یک یا چند بلوک است که معمولاً «انتخاب» یا «فیلتر» نامیده می شود، اما می تواند هر نام دیگری داشته باشد.
- هر بلوک حاوی فیلد ها و اطلاعات مربوطه است که برای تشخیص یک رویداد خاص مورد نیاز است.
- هنگامی که به دنبال یک مطابقت می گردیم، می توانیم با استفاده از فیلد ها و ویژگی های زیر به دنبال یک رشته خاص، شناسه رویداد یا ترکیبی از آنها باشیم.

- ```
{
 "keywords": [
 "org.apache.commons.ognl.OgnlException",
 "ExpressionSyntaxException"
],
 "condition": "keywords"
},
{
 "keywords": [
 "Cannot run program",
 "java.lang.ProcessImpl",
 "java.lang.ProcessBuilder"
],
 "condition": "keywords"
},
```
- انتخاب ها: شناسه ها را برای داده های گزارش جستجو می کند
  - شرایط: نحوه ارزیابی انتخاب یا فیلترها را مشخص می کند

# Sigma rules

## detection

```
detection:
 selection:
 Provider_Name|startswith:
 - "Microsoft"
 - "Micr"
 Computer: "BelkaVirtualDev"
 filter:
 Channel:
 - "Setup"
 - "System"
 condition: selection and filter
```

- گره از مجموعه ای از زیرگره ها تشکیل شده است که هر کدام شرطی را بر خاصیت خاصی تحمیل می کنند. به عنوان مثال، گره "انتخاب" در تصویر بالا، یک فیلتر برای نام ارائه دهنده (یعنی نام منبع) و ویژگی های کامپیوتر اعمال می کند.

# Sigma rules

```
detection:
 selection:
 Provider_Name|startswith:
 - "Microsoft"
 - "Micr"
 Computer: "BelkaVirtualDev"
filter:
 channel:
 - "Setup"
 - "System"
condition: selection and filter
```

```
node1:
 node11:
 node111:
 - "Microsoft"
 - "Micr"
 node112:
 - "Some value"
 node12: "BelkaVirtualDev"
node2:
 - "Micr"
 - ""
```

## detection

### انواع گره :

- **Mapping node** نود کامپیوتر که شامل کلید و مقدار میشود.
- **Sequence node** نود که باید مقداری برابر system setup یا channel داشته باشد.
- **Complex node** نود چندین نود دیگر است.

```
(
 (
 (node111 = "Microsoft" OR node111 = "Micr")
 AND
 (node112 = "Some value")
)
 AND
 node12 = "BelkaVirtualDev"
)
AND
(node2 = "Micr" OR node2 = "")
```

# Sigma rules

## detection

انواع گره :

```
detection:
 selection:
 Provider_Name|startswith:
 - "Microsoft"
 - "Micr"
 Computer: "BelkaVirtualDev"
 filter:
 Channel:
 - "Setup"
 - "System"
 condition: selection and filter
```

(Provider\_Name starts\_with "Microsoft" OR Provider\_Name starts\_with "Micr")  
AND  
Computer = "BelkaVirtualDev"  
AND  
(Channel = "Setup" OR Channel = "System")  
.

```
node1:
 node11:
 node111:
 - "Microsoft"
 - "Micr"
 node112:
 - "Some value"
 node12: "BelkaVirtualDev"
node2:
 - "Micr"
 - ""
```

# Sigma rules

## detection

| Sections  | Attributes     |
|-----------|----------------|
|           | title          |
|           | id             |
|           | status         |
|           | author         |
|           | date           |
|           | modified       |
| Metadata  | description    |
|           | references     |
|           | tags           |
|           | falsepositives |
|           | level          |
| Logsource | logsource      |
|           | category       |
|           | product        |
|           | service        |
|           | definition     |
|           | detection      |
| Detection |                |
|           | condition      |

```
logsource:
category: process_creation
product: windows

detection:
selection:
 ParentImage|endswith:
 - '\svchost.exe'
 - 'cmd.exe'
 - 'powershell.exe'
 Image|endswith:
 - '\mshta.exe'
condition: selection
```

- بررسی یک مثال در این فیلد:
- این قانون می تواند برای اسکن گزارش های ایجاد فرآیند در سیستم عامل ویندوز استفاده شود.
- در بلوک "انتخاب" که یک نقشه (یا دایرکتوری) است که شامل جفت کلید و مقادیر است.
- در مثال بالا دو کلید وجود دارد: "ParentImage" و "Image". " و " AND منطقی مرتبط هستند.
- عناصر نقشه با AND منطقی مرتبط هستند.
- این معنی است که ما به دنبال تطبیقی برای تصویر فرآیند و تصویر والد آن هستیم.
- برای تصویر والد رشته ها در قالب لیست هستند. آنها با OR مرتبط هستند و ما به حداقل ۱ مطابقت نیاز داریم:
- در این قسمت می توان از عبارات منظم regular expressions نیز استفاده کرد.
- یا اصلاح کننده، این قسمت در این مثال برابر endwith می باشد که مشخص می کند مقادیر لیست در کدام قسمت باید جست و جو شوند.

# Sigma rules

## detection

کامپایل قانون به زبان های splunk , sqlite

| Sections  | Attributes     |
|-----------|----------------|
|           | title          |
|           | id             |
|           | status         |
|           | author         |
|           | date           |
|           | modified       |
| Metadata  | description    |
|           | references     |
|           | tags           |
|           | falsepositives |
|           | level          |
| Logsource | logsource      |
|           | category       |
|           | product        |
|           | service        |
|           | definition     |
|           | detection      |
| Detection |                |
|           | condition      |

```
logsource:
category: process_creation
product: windows
detection:
selection:
ParentImage|endswith:
- '\svchost.exe'
- 'cmd.exe'
- 'powershell.exe'
Image|endswith:
- '\mshta.exe'
condition: selection
```

```
./sigmac -t splunk -c config/generic/windows-services.yml
sigma_rules/detect_mshta.yml
((ParentImage="*\svchost.exe" OR ParentImage="*cmd.exe" OR
ParentImage="*powershell.exe") (Image="*\mshta.exe"))
```

```
./sigmac -t sqlite -c config/generic/windows-services.yml
sigma_rules/detect_mshta.yml
SELECT * FROM eventlog WHERE ((ParentImage LIKE '%\svchost.exe' ESCAPE '\\'
OR ParentImage LIKE '%cmd.exe' ESCAPE '\\' OR ParentImage LIKE
'%powershell.exe' ESCAPE '\\') AND (Image LIKE '%\mshta.exe' ESCAPE '\\'))
```

# Sigma rules

## condition

| Sections  | Attributes     |
|-----------|----------------|
| Metadata  | title          |
|           | id             |
|           | status         |
|           | author         |
|           | date           |
|           | modified       |
|           | description    |
|           | references     |
|           | tags           |
|           | falsepositives |
| Logsource | level          |
|           | logsource      |
|           | category       |
|           | product        |
|           | service        |
| detection | definition     |
|           | detection      |
| Detection | condition      |

◦ در این فیلد، **مجموعه شرایط** یا **همان معیارها یا الگوهای خاصی** که قانون به دنبال آن است قرار می‌گیرند.

◦ گره‌های سطح بالا در عبارت منطقی نهایی شرکت می‌کنند که با کلید "شرط" و یک عبارت منطقی، به عنوان مثال، "شرط: انتخاب و فیلتر" تعریف می‌شود.

"condition: selection and filter". ◦

◦ یک قانون همچنین می‌تواند شامل عملگر "نه" باشد، به عنوان مثال، "شرط: کلمات کلیدی و نه فیلتر".

"condition: keywords and not filter". ◦

# detection

```
1
2 ### Search Identifier, Condition Example
3
4 detection:
5 selection1:
6 Image|endswith:
7 - 'cmd.exe'
8 - 'powershell.exe'
9 selection2:
10 ParentImage|endswith:
11 - 'winword.exe'
12 - 'excel.exe'
13 - 'powerpnt.exe'
14
15 condition: selection1 AND selection2
```

The diagram illustrates the structure of a detection rule. It consists of several nested sections:

- Detection Attribute:** The outermost section, labeled 'detection'.
- Search-Identifiers:** Two sub-sections within the 'detection' attribute: 'selection1' and 'selection2'. These are represented by yellow boxes.
- Condition Attribute:** A final section at the bottom labeled 'condition'.

Annotations with arrows point to each of these three main components:

- An arrow points from the label 'Detection Attribute' to the 'detection:' line.
- An arrow points from the label 'Search-Identifiers' to the 'selection1:' and 'selection2:' lines.
- An arrow points from the label 'Condition Attribute' to the 'condition:' line.

Detection Attribute Section

# Sigma rules

## detection

### LISTS:

اگلباً یک علامت خط تیره "—" نشان داده می شود که به معنای "OR" منطقی است، انتخاب می تواند هر تعداد عنصر در یک لیست داشته باشد، همه با "OR" منطقی به هم متصل می شوند.

```
LISTS Example
detection:
 selection:
 ParentImage|endswith:
 - '\cmd.exe'
 - '\powershell.exe'
 condition: selection
```

### MAPS:

جفت های Key-Value هستند، که در آن «Key» نام فیلد داده های گزارش است، و «Value» مقدار داده (رشته / عدد صحیح) در داده های گزارش داده شده است، انتخاب می تواند هر تعداد جفت کلید-مقدار داشته باشد، همه با "AND" منطقی پیوست می شوند

```
MAPS Example
detection:
 selection:
 Image|endswith: '\wmic.exe'
 CommandLine|contains: '/node:'
 condition: selection
```

# Sigma rules detection

## LISTS & MAPS

```
2 ### Search Identifier Example, Type: List
3 detection:
4 selection:
5 Image|endswith:
6 - 'cmd.exe'
7 - 'powershell.exe'
8 ParentImage|endswith:
9 - 'winword.exe'
10 - 'excel.exe'
11 - 'powerpnt.exe'
12 condition: selection
13
14 ### Search Identifier Example, Type: Maps
15 detection:
16 selection:
17 Image|endswith: '\wmic.exe'
18 CommandLine|contains: '/node:'
19 condition: selection
20
21
```

### List

Elements in a list begin with "-" dash bullet and are linked with logical 'OR'

#### Condition Matches:

(Image == 'cmd.exe' OR Image == 'powershell.exe') AND  
(ParentImage == 'winword.exe' OR ParentImage ==  
'excel.exe' OR ParentImage == 'powerpnt.exe')

### Maps (Key-Value Pair)

Key is the field name from the log data or event  
Value can be String/Integer value searching for  
Elements are linked with Logical 'AND'

#### Condition Matches:

(Image == 'wmic.exe' AND CommandLine == '/node:')

# Sigma rules

## detection

### Value Modifiers

| Value Modifier | What changes, when value modifiers are used          | Example                  |
|----------------|------------------------------------------------------|--------------------------|
| endswith       | Adds '*' to the beginning of the field value         | ParentImage endswith     |
| startswith     | Adds '*' to the end of the field value               | Image startswith         |
| contains       | Adds '*' to beginning & end of the field value       | CommandLine contains     |
| all            | Changes the default list behavior from 'or' to 'and' | CommandLine contains all |

Sigma rules

detection

## Condition Expression

| Condition Operators        | Example                                      |
|----------------------------|----------------------------------------------|
| Logical operators AND/OR   | selection1 OR selection2                     |
| 1/all of search-identifier | 1 of selection*                              |
| 1/all of them              | all of them                                  |
| Negation with 'NOT'        | selection1 AND NOT filter                    |
| Order of operation '()'    | 1 of selection* AND NOT (filter1 or filter2) |

# Sigma rules

## detection

### Logical "OR"

```
Example-1 Condition with Logical "OR"
title: Suspicious 'mshta.exe' Process Executions via Command Line tools
detection:
 selection1:
 EventID: 7045
 ServiceName: 'PSEXESVC'
 ServiceFileName: '\PSEXESVC.exe'
 selection2:
 EventID: 7036
 ServiceName: 'PSEXESVC'
 selection3:
 EventID: 1
 Image: '*\PSEXESVC.exe'
 User: 'NT AUTHORITY\SYSTEM'
Condition: selection1 OR selection2 OR selection3
```

**evaluates and matches to** (EventID == 7045 AND ServiceName == 'PSEXESVC' AND ServiceFileName == '\PSEXESVC.exe') OR (EventID == 7036 AND ServiceName == 'PSEXESVC') OR (EventID == 1 AND Image == '\* \PSEXESVC.exe' AND User == 'NT AUTHORITY\SYSTEM')

Operators (1/any of Search-Identifiers)

1 of selection\*

1 of them

any of selection\*

# Sigma rules

## detection

### Logical "AND"

```
Example-2 Condition with Logical "AND"
title: Suspicious 'mshta.exe' Process Executions via Command Line tools
detection:
 selection1:
 Image: '*\mshta.exe'
 selection2:
 ParentImage:
 - '*\cmd.exe'
 - '*\powershell.exe'
condition: selection1 AND selection2
```

```
Image == '*\ mshta.exe' AND (ParentImage == '* \cmd.exe' or ParentImage ==
'*\powershell.exe')
```

Operators (all of search-identifier)

all of selection\*

all of them

# Sigma rules detection

## Negation with "NOT"

```
Example-3 Condition with Negation with "NOT"
title: 'mshta.exe' process execution from untrusted locations
detection:
 selection:
 Image|endswith: '\mshta.exe'
 filter:
 Image|contains:
 - 'C:\Windows\System32'
 - 'C:\Windows\SysWOW64'
 condition: selection AND NOT filter
```

```
Image == '*\mshta.exe' AND NOT (Image == 'C:\Windows\System32' or Image ==
'C:\Windows\SysWOW64')
```

# Sigma rules detection

## “AND/OR”

```
Example-4 Condition with Negation with "AND/OR"
title: Suspicious 'mshta.exe' Process Executions
detection:
 selection1:
 Image|endswith: '\mshta.exe'
 selection2:
 ParentImage|endswith:
 - '\cmd.exe'
 - '\powershell.exe'
 selection3:
 CommandLine|contains:
 - '\AppData\Local'
 - 'C:\Windows\Temp'
 - 'C:\Users\Public'
 condition: selection1 AND (selection2 OR selection3)
```

**evaluates and matches to** Image == '\* \mshta.exe' AND ((ParentImage == '\* \cmd.exe'  
or ParentImage == '\*\powershell.exe') OR (CommandLine == '\*\AppData\Local\*' or  
CommandLine == '\*C:\Windows\Temp\*' or CommandLine == '\*C:\Users\Public\*'))

# Sigma rules detection

```
title: Suspicious Execution of 'MSHTA.exe' Process
detection:
Binary
selection_base:
 Image|endswith: '\mshta.exe'
Suspicious parents
selection1:
 ParentImage|endswith:
 - '\cmd.exe'
 - '\powershell.exe'
Suspicious folders
selection2:
 CommandLine|contains:
 - '\AppData\Local'
 - 'C:\Windows\Temp'
 - 'C:\Users\Public'
Suspicious Execution Locations
filter1:
 Image|contains:
 - 'C:\Windows\System32'
 - 'C:\Windows\SysWOW64'
filter2:
 CommandLine|contains:
 - '.htm'
 - '.hta'
 CommandLine|endswith:
 - 'mshta.exe'
 - 'mshta'
condition: selection_base and (selection1 or selection2) or
(selection_base and not filter1) or (selection_base and not filter2)
```

# Sigma rules detection

```
detection:
 # Binary Selector
 selection_base:
 Image|endswith: '\mshta.exe'
 # Suspicious parents
 selection1:
 ParentImage|endswith:
 - '\cmd.exe'
 - '\powershell.exe'
 # Suspicious folders
 selection2:
 CommandLine|contains:
 - '\AppData\Local'
 - 'C:\Windows\Temp'
 - 'C:\Users\Public'
 # Suspicious Execution Locations
 filter1:
 Image|contains:
 - 'C:\Windows\System32'
 - 'C:\Windows\SysWOW64'
 # Suspicious extensions
 filter2:
 CommandLine|contains:
 - '.htm'
 - '.hta'
 CommandLine|endswith:
 - 'mshta.exe'
 - 'mshta'

condition: selection_base and (selection1 or selection2) or (selection_base and not filter1) or (selection_base and not filter2)
```

Search Identifiers

Condition

# Sigma rules detection

```
title: Suspicious Execution of 'MSHTA.exe' Process
detection:
Binary
selection_base:
 Image|endswith: '\mshta.exe'
Suspicious parents
selection1:
 ParentImage|endswith:
 - '\cmd.exe'
 - '\powershell.exe'
Suspicious folders
selection2:
 CommandLine|contains:
 - '\AppData\Local'
 - 'C:\Windows\Temp'
 - 'C:\Users\Public'
Suspicious Execution Locations
filter1:
 Image|contains:
 - 'C:\Windows\System32'
 - 'C:\Windows\SysWOW64'
filter2:
 CommandLine|contains:
 - '.htm'
 - '.hta'
 CommandLine|endswith:
 - 'mshta.exe'
 - 'mshta'
condition: selection_base and (selection1 or selection2) or
(selection_base and not filter1) or (selection_base and not filter2)
```

**evaluates and matches to** (Image == '\mshta.exe' AND ((ParentImage == '\cmd.exe' or ParentImage == '\powershell.exe') OR (CommandLine == '\AppData\Local' or CommandLine == 'C:\Windows\Temp' or CommandLine == 'C:\Users\Public'))) OR (Image == '\mshta.exe' AND NOT (Image == 'C:\Windows\System32' or Image == 'C:\Windows\SysWOW64')) OR (Image == '\*\mshta.exe' AND NOT ((CommandLine == '.htm' or CommandLine == '.hta') AND (CommandLine == 'mshta.exe' or CommandLine == 'mshta'))))

# Sigma rules detection

```
detection:
 selection1:
 ParentImage|endswith:
 - '\winlogon.exe'
 - '\services.exe'
 - '\lsass.exe'
 - '\csrss.exe'
 - '\smss.exe'
 - '\wininit.exe'
 - '\spoolsv.exe'
 - '\searchindexer.exe'
 selection2:
 Image|endswith:
 - '\powershell.exe'
 - '\cmd.exe'
 selection3:
 User|contains: # covers many language settings
 - "AUTHORI"
 - "AUTORI"
 filter:
 CommandLine|contains|all:
 - " route "
 - " ADD "
 condition: selection1 and selection2 and selection3 and not filter
fields:
 - ParentImage
 - Image
 - User
 - CommandLine
```

در مثال زیر، اگر شرایط `\selection1`، `\selection2` و `\selection3` فعال شوند و هیچ مطابقتی برای فیلتر وجود نداشته باشد، یک تطابق رخ خواهد داد.

# 1.Single Search Identifier

```
detection:
 search_identifier_1:
 CommandLine:
 - DumpCreds
 - invoke-mimikatz
 condition: search_identifier_1
```

## 2. Logical AND/OR

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
condition: search_identifier_1 and search_identifier_2
```

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
condition: search_identifier_1 or search_identifier_2
```

### 3. Negation with 'not'

```
detection:
 search_identifier_1:
 EventID: 4738
 search_identifier_2:
 PasswordLastSet: null
 condition: search_identifier_1 and not search_identifier_2
```

## 4. x of Search Identifier

```
detection:
 search_identifier_1|contains:
 - EVILSERVICE
 - svchost.exe -n evil
 search_identifier_2|contains:
 - token
 - rpc
 - crypto
condition: 2 of search_identifier_1 and search_identifier_2
```

```
detection:
 search_identifier_1:
 - EVILSERVICE
 - svchost.exe -n evil
 search_identifier_2:
 - token
 - rpc
 - crypto
condition: all of search_identifier_1 and 2 of search_identifier_2
```

## 5. x of them

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
 - crypto
 search_identifier_3:
 CommandLine|contains:
 - bitcoin
condition: 1 of them
```

## 6. x of Search Identifier Pattern

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
 - crypto
 search_identifier_3:
 CommandLine|contains:
 - bitcoin
condition: all of search_identifier_*
```

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
 - crypto
 log_filter_1:
 PasswordLastSet: null
 log_filter_2:
 Username: null
condition: 1 of search_identifier_* and not 1 of log_filter_*
```

## 7. Brackets (and condition precedence)

```
detection:
 search_identifier_1:
 CommandLine|contains:
 - DumpCreds
 - invoke-mimikatz
 search_identifier_2:
 CommandLine|contains:
 - rpc
 - token
 - crypto
 search_identifier_3:
 CommandLine|contains:
 - bitcoin
condition: (search_identifier_1 and search_identifier_2) or
 (search_identifier_2 and search_identifier_3) and not
 (search_identifier_1 and search_identifier_3)
```

- هر ترکیبی به جز و search\_identifier\_1 باعث search\_identifier\_3 شناسایی می‌شوند.

# keywords

```
detection:
 keywords:
 - "tftp"
 - "rcp"
 - "puts"
 - "copy"
 - "configure replace"
 - "archive tar"
condition: keywords
```

- این فیلد نشان می دهد که ایا مقادیر لیست رو به رو در **event text** یا **description** گزارش وجود دارد یا خیر.

# Sigma rules

| Sections  | Attributes     |
|-----------|----------------|
| Metadata  | title          |
|           | id             |
|           | status         |
|           | author         |
|           | date           |
|           | modified       |
| Logsource | description    |
|           | references     |
|           | tags           |
| Logsource | falsepositives |
|           | level          |
|           | logsource      |
|           | category       |
|           | product        |
|           | service        |
| Detection | definition     |
|           | detection      |
| Condition |                |
|           | condition      |

- این فیلد، شامل یک آی دی و پورت می شود.
- ارتباط با سایر قانون ها را بررسی می کند.

```
[
 {
 "id": "6897cd82-6664-11ed-9022-0242ac120002",
 "type": "similar"
 },
 [
 {
 "id": "18b88d08-d73e-4f21-bc25-4b9892a4fdd0",
 "type": "similar"
 }
]
]
```

# Sigma rules

| Sections  | Attributes                          |
|-----------|-------------------------------------|
| Metadata  | title                               |
|           | id                                  |
|           | status                              |
|           | author                              |
|           | date                                |
|           | modified                            |
|           | description                         |
|           | references                          |
|           | tags                                |
| Logsource | falsepositives                      |
|           | level                               |
|           | logsource                           |
|           | category                            |
|           | product                             |
|           | service                             |
| Detection | definition                          |
|           | detection                           |
|           | filename                            |
|           | computername                        |
|           | user                                |
|           | userIdentity.arn                    |
|           | responseElements.accessKey.userName |
|           | errorCode                           |
|           | errorMessage                        |
| Condition | sourceIPAddress                     |
|           | requestParameters.userName          |

اینها زمینه هایی هستند که در ارزیابی یک رویداد خاص بسیار کمک کننده هستند.  
به عنوان مثال، دانستن فرآیند والد فرآیندی که شامل رشته های مشکوک در پارامترهای خط فرمان است، مفید است.  
این فیلدها می توانند به صورت خودکار استخراج شوند و به تحلیلگر ارائه شوند تا سرعت تجزیه و تحلیل افزایش یابد.

## fields

: نام فایل مرتبط با رویداد یا لاگ.

: نام کاربری مرتبط با رویداد یا لاگ.

: امضا یا توصیفی از رویداد یا فایل مرتبط.

: نام کامپیوتر یا سرور مرتبط با رویداد یا لاگ.

: شناسه یکتای مرتبط با هویت کاربری.

: نام کاربری مرتبط با دسترسی کلید.

: کد و پیام خطأ مرتبط با رویداد.

: آدرس IP منبع مرتبط با رویداد یا لاگ.

# Sigma rules

| Sections  | Attributes     |
|-----------|----------------|
| Metadata  | title          |
|           | id             |
|           | status         |
|           | author         |
|           | date           |
|           | modified       |
|           | description    |
|           | references     |
| Logsource | tags           |
|           | falsepositives |
|           | level          |
|           | logsource      |
|           | category       |
| Detection | product        |
|           | service        |
|           | definition     |
|           | detection      |
| Condition |                |

## license

- این فیلد نشان می دهد که آیا می توان از قانون استفاده کرد. مشروط بر این که نویسنده این قانون را به اشتراک گذاشته باشد.
- وجود این فیلد در قوانین سیگما اختیاری است.

# بررسی یک قانون سیگما

title: Credential Dumping via SharpSecDump Tool  
status: experimental  
  
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool, ported from python/impacket to .net. This technique is commonly utilized for credential dumping. Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.  
author: Picus Security  
  
references:  
- <https://attack.mitre.org/tactics/TA0006/>  
- <https://attack.mitre.org/techniques/T1003/>  
- <https://github.com/G0ldenGunSec/SharpSecDump>  
  
logsource:  
product: windows  
service: security  
  
definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation'  
  
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\ System\ Audit Process Creation\ Include Command Line'  
  
detection:  
selection:  
    EventID: 4688  
    ProcessCommandLine: "\*sharpsecdump\*"  
condition: selection  
  
falsepositives:  
- Unknown  
  
level: high  
  
tags:  
- attack.credential\_access  
- attack.ta0006

Code 1. An Example Sigma Rule Developed by Picus Security

title: Credential Dumping via SharpSecDump Tool

عنوان نشان می دهد که هدف این قانون  
شناسایی Dumping اعتبار با استفاده  
از ابزاری به نام SharpSecDump است.

status

title: Credential Dumping via SharpSecDump Tool  
status: experimental  
  
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool, ported from python/impacket to .net. This technique is commonly utilized for credential dumping. Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.  
author: Picus Security  
  
references:  
- <https://attack.mitre.org/tactics/TA0006/>  
- <https://attack.mitre.org/techniques/T1003/>  
- <https://github.com/G0ldenGunSec/SharpSecDump>  
  
logsource:  
product: windows  
service: security  
  
definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation'  
  
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\System\ Audit Process Creation\ Include Command Line'  
  
detection:  
selection:  
    EventID: 4688  
    ProcessCommandLine: "\*sharpsecdump\*"  
condition: selection  
  
falsepositives:  
- Unknown  
  
level: high  
  
tags:  
- attack.credential\_access  
- attack.ta0006

status: experimental

وضعیت "تجربی" است، به این معنی که این قانون در مرحله آزمایش است و ممکن است هنوز در یک محیط تولید قابل اطمینان نباشد.

Code 1. An Example Sigma Rule Developed by Picus Security



# Description

title: Credential Dumping via SharpSecDump Tool

status: experimental

d  
c  
n  
a  
n  
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool,  
ported from python/impacket to .net. This technique is commonly utilized for credential  
dumping. Adversaries may attempt to dump credentials to obtain account login and credential  
material, normally in the form of a hash or a clear text password, from the operating system  
and software.

Command Line:

detection:

selection:

EventID: 4688

ProcessCommandLine: "\*sharpsecdump\*

condition: selection

falsepositives:

- Unknown

level: high

tags:

- attack.credential\_access

- attack.ta0006

این زمینه بیشتری را فراهم می کند. این هدف دشمنان را در استفاده از SharpSecDump توصیف می کند - **برای حذف اعتبار حساب های معتبر**، چه به صورت هش شده یا متن ساده.

Code 1. An Example Sigma Rule Developed by Picus Security

title: Credential Dumping via SharpSecDump Tool  
status: experimental  
  
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool, ported from python/impacket to .net. This technique is commonly utilized for credential dumping. Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.  
  
author: Picus Security  
  
references:  

- <https://attack.mitre.org/tactics/TA0006/>
- <https://attack.mitre.org/techniques/T1003/>
- <https://github.com/G0ldenGunSec/SharpSecDump>

  
logsource:  
  
product: windows  
  
service: security  
  
definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation'  
  
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\ System\ Audit Process Creation\ Include Command Line'  
  
detection:  
  
selection:  

- EventID: 4688
- ProcessCommandLine: "\*sharpsecdump\*

  
condition: selection  
  
falsepositives:  

- Unknown

  
level: high  
  
tags:  

- attack.credential\_access
- attack.ta0006

Code 1. An Example Sigma Rule Developed by Picus Security

# Author and References

author: Picus Security

references:

- <https://attack.mitre.org/tactics/TA0006/>
- <https://attack.mitre.org/techniques/T1003/>
- <https://github.com/G0ldenGunSec/SharpSecDump>

این قانون توسط **Picus Security** نوشته شده است. ارجاع‌ها به منابعی پیوند می‌خورند، که به اثبات تکنیک مورد اشاره در قانون کمک می‌کند و **اطلاعات بیشتری** در مورد تهدید ارائه می‌کند.

## Logsource

```
logsource:

product: windows

service: security

definition1: 'Requirements: Group Policy : Computer Configuration\Windows
Settings\Security Settings\Advanced Audit Policy Configuration\Audit
Policies\Detailed Tracking\Audit Process Creation'

definition2: 'Requirements: Group Policy : Computer Configuration\
Administrative Templates\System\ Audit Process Creation\ Include
Command Line'
```

هر قانون سیگما باید منابع گزارش هایی را که تجزیه و تحلیل می کند مشخص کند. این قانون خاص برای خواندن گزارش ها از سرویس امنیتی در سیستم های ویندوز طراحی شده است.

## Definitions

آنها تنظیمات حسابرسی لازم برای ایجاد رویدادهای گزارش مورد نیاز برای عملکرد صحیح این قانون تشخیص را تشریح می کنند.

تنظیم خط مشی گروه برای ایجاد فرآیند حسابرسی

## Detection

detection:

selection:

EventID: 4688

ProcessCommandLine: '\*sharpsecdump\*'

condition: selection

'نشان دهنده رویداد خاص ویندوز است که EventID' قانون در آن جستجو می کند. '۴۶۸۸' مربوط به رویدادی است که در آن یک فرآیند جدید ایجاد شده است.

'ProcessCommandLine' نشان دهنده دستور دقیقی است که برای مقداردهی اولیه برنامه مورد نظر استفاده می شود.

تشخیص 'sharpsecdump' در ProcessCommandLine استنباط می کند که SharpSecDump ابزار اجرا شده است.

## False Positives

falsepositives:

- Unknown

هیچ قانونی ایمن نیست. در حالی که فهرست مشخصی از سناریوها وجود ندارد که می‌تواند به نتایج مثبت کاذب منجر شود، شناخت احتمالات چنین رخدادهایی به تحلیلگران کمک می‌کند تا هنگام ایجاد هشدارها از قضاوت خود استفاده کنند.

```
title: Credential Dumping via SharpSecDump Tool
status: experimental
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool, ported from python/impacket to .net. This technique is commonly utilized for credential dumping. Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.
author: Picus Security
references:
- https://attack.mitre.org/tactics/TA0006/
- https://attack.mitre.org/techniques/T1003/
- https://github.com/G0ldenGunSec/SharpSecDump
logsource:
product: windows
service: security
definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation'
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\System\ Audit Process Creation\ Include Command Line'
detection:
selection:
EventID: 4688
ProcessCommandLine: "*sharpsecdump*"
condition: selection
falsepositives:
- Unknown
level: high
tags:
- attack.credential_access
- attack.ta0006
```

Code 1. An Example Sigma Rule Developed by Picus Security

level: high

"بالا" نشان می دهد که این قانون برای یافتن تهدیدهای امنیتی جدی است. هشدارهای ایجاد شده توسط این قانون باید نسبت به هشدارهایی که در سطوح متوسط یا پایین هستند اولویت داشته باشند.

# Tags

title: Credential Dumping via SharpSecDump Tool  
status: experimental  
  
description: Detects the attempt of SharpSecDump usage, a credential harvesting tool, ported from python/impacket to .net. This technique is commonly utilized for credential dumping. Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software.  
  
author: Picus Security  
  
references:  
- <https://attack.mitre.org/tactics/TA0006/>  
- <https://attack.mitre.org/techniques/T1003/>  
- <https://github.com/G0ldenGunSec/SharpSecDump>  
  
logsource:  
  
product: windows  
  
service: security  
  
definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation'  
  
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\System\ Audit Process Creation\ Include Command Line'  
  
detection:  
  
selection:  
    EventID: 4688  
    ProcessCommandLine: "\*sharpsecdump\*"  
  
condition: selection  
  
falsepositives:  
- Unknown  
  
level: high  
  
tags:  
- attack.credential\_access  
- attack.ta0006

## tags:

- attack.credential\_access
- attack.ta0006

آنها با نگاشت به تکنیک های حمله سایبری شناخته شده، این قانون را دسته بندی می کنند.  
'attack.credential\_access' تاکتیک Credential Access در MITER ATT&CK قرار چارچوب می گیرد که نشان می دهد این قانون با هدف شناسایی تلاش ها برای سرقت اعتبارنامه های ورود است.

| Sigma rule for log files where `$_raw` is for network traffic and `DATA` is for files

```
title: Webshell ReGeorg Detection Via Web Logs
id: 2ea44a60-cfda-11ea-87d0-0242ac130003
status: test
description: >
 Certain strings in the uri_query field when combined with
 null referer and null user agent can indicate activity
 associated with the webshell ReGeorg.
references:
 - https://community.rsa.com/community/products/netwitness/blog/2019/02/19/
 - https://github.com/sensepost/reGeorg
author: Cian Heasley
date: 2020/08/04
modified: 2023/01/02
tags:
 - attack.persistence
 - attack.t1505.003
logsource:
 category: webserver
detection:
 selection:
 cs-uri-query|contains:
 - 'cmd=read'
 - 'connect&target'
 - 'cmd=connect'
 - 'cmd=disconnect'
 - 'cmd=forward'
 filter:
 cs-referer: null
 cs-user-agent: null
 cs-method: POST
 condition: selection and filter
falsepositives:
 - Web applications that use the same URL parameters as ReGeorg
fields:
```

```
(cs-uri-query LIKE '%cmd=read%'
OR cs-uri-query LIKE '%connect&target%'
OR cs-uri-query LIKE '%cmd=connect%'
OR cs-uri-query LIKE '%cmd=disconnect%'
OR cs-uri-query LIKE '%cmd=forward%')
AND (cs-referer IS NULL
AND cs-USER-agent IS NULL
AND cs-METHOD LIKE 'POST'))
```

# اعمال تجمعی زمانی توسط قوانین سیگما

```
detection:
 selection:
 EventID: 5156
 DestPort:
 - 3268
 - 3269
 timeframe: 1h
 condition: selection | count() by SourceAddress > 2000
```

- شمارش از طریق کاتالوگ جهانی
- کوئری روبه رو بارها و بارها اجرا می شود و تعداد رویدادهای یکسان را بارها و بارها پردازش بررسی می شود.  
هر بار شمارنده به روزرسانی می کند.

## همبستگی شمارش.

: Count() by Y

نمونه های منحصر به فرد مقدار فیلد Y را می شمارد و (بزرگتر از، کمتر از) آن را با یک عدد ثابت مقایسه می کند.

Count() by src\_ip > 2 مثال:

:Count(X) by Y

نمونه های منحصر به فرد مقدار فیلد X را به ازای هر مقدار Y می شمارد و تعداد X را با یک عدد ثابت مقایسه می کند.

Count(EventID) by src\_ip > 2

## همبستگی شمارش.

Count() by src\_ip > 10

تطبیق های منحصر به فرد بر اساس آی پی مبدا

Count() by dst\_ip > 10

تطبیق های منحصر به فرد بر اساس آی پی مقصد

Count(EventID) by ComputerName

شمارش نمونه های منحصر به فرد EVENT ID؛، برای مثال با شمارش ای دی یک رخداد منحصر به فرد می توان تشخیص داد که آیا این رخداد در یک زمان مشخص شروع و خاتمه یافته است یا خیر

| SIGMA detection component                                                                                                        | Splunk Translation (Asterisk is a wildcard)                                 |                             |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------|
| <pre>detection: selection:   fieldX: 'suspicious' condition: selection</pre>                                                     | fieldX="suspicious"                                                         | <h1>SIGMA &amp; SPLUNK</h1> |
| <pre>detection: selection:   fieldY contains:     - 'suspicious'     - 'malicious'     - 'pernicious' condition: selection</pre> | (fieldY="*suspicious*" OR<br>fieldY="*malicious*" OR fieldY="*pernicious*") |                             |
| <pre>detection: selection:   - fieldX: 'icious'   - fieldX:     - 'susp'     - 'mal'     - 'pern' condition: selection</pre>     | (FieldX="icious" AND (FieldX="susp" OR<br>FieldX="mal" OR FieldX="pern"))   |                             |

detection:  
selection:  
- FieldX|endswith: 'icious'  
- FieldX|startswith:  
  - 'susp'  
  - 'mal'  
  - 'pern'

(FieldX="\*icious" AND (FieldX="susp\*" OR  
FieldX="mal\*" OR FieldX="pern\*"))

condition: selection

detection:  
selection:  
FieldX|endswith: 'icious'  
filter:  
FieldX|startswith:  
  - 'del'  
  - 'ausp'

(FieldX="\*icious" AND NOT ((FieldX="del\*"  
OR FieldX="ausp\*")))

condition: selection AND NOT filter

detection:  
selection:  
FieldX: 'suspicious'  
timeframe: 1m  
condition: selection | count by src\_ip > 3

FieldX="suspicious" | eventstats count as val  
by src\_ip| search val > 3  
#notice splunk ignores the timeframe value,  
the value must be set at search by the user

# SIGMA & SPLUNK

# Sigma Rules Structure

| Sections  | Attributes     | Value (Example)                                                                                                                                                                                                                                                                                | Remark    |
|-----------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Metadata  | title          | Installation of Malicious Service                                                                                                                                                                                                                                                              | Mandatory |
|           | id             | 2cfe636e-317a-4bee-9f2c-1066d9f54d1a                                                                                                                                                                                                                                                           |           |
|           | status         | stable                                                                                                                                                                                                                                                                                         |           |
|           | author         | Blusapphire, SOC                                                                                                                                                                                                                                                                               |           |
|           | date           | 2017/03/27                                                                                                                                                                                                                                                                                     |           |
|           | modified       | 2021/07/06                                                                                                                                                                                                                                                                                     |           |
|           | description    | Detects known malicious service installs that only appear in cases of lateral movement, credential dumping, and other suspicious activities.                                                                                                                                                   | Optional  |
|           | references     | - <a href="https://awakesecurity.com/blog/threat-hunting-for-paexec/">https://awakesecurity.com/blog/threat-hunting-for-paexec/</a><br>- <a href="https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf">https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf</a> |           |
|           | tags           | - attack.t1035<br>- attack.t1050                                                                                                                                                                                                                                                               |           |
| Logsource | falsepositives | - Penetration testing                                                                                                                                                                                                                                                                          |           |
|           | level          | critical                                                                                                                                                                                                                                                                                       |           |
|           | logsource      |                                                                                                                                                                                                                                                                                                | Mandatory |
|           | category       |                                                                                                                                                                                                                                                                                                |           |
|           | product        | windows                                                                                                                                                                                                                                                                                        |           |
| Detection | service        | system                                                                                                                                                                                                                                                                                         | Optional  |
|           | definition     |                                                                                                                                                                                                                                                                                                |           |
|           | detection      |                                                                                                                                                                                                                                                                                                |           |
|           |                | selection:<br>EventID: 7045<br>malsvc_paexec:<br>ServiceFileName contains: '\PAExec'<br>malsvc_wannacry:<br>ServiceName: 'mssecsvc2.0'<br>malsvc_persistence:<br>ServiceFileName contains: 'net user'                                                                                          | Mandatory |
|           | condition      | selection and (malsvc_paexec or malsvc_wannacry or malsvc_persistence)                                                                                                                                                                                                                         |           |