

徹底解説! まだ知られていないFalcon便利機能!

2018/12/11 マクニカネットワークス株式会社 技術統括部 第6技術部 第2課





Copyright © 2004-2018 Macnica Networks Corp. All Rights Reserved.

ご紹介内容



運用に活用できる小ネタ集
 アラートのフィルタリング・グルーピング表示切替
 アラートステータス・担当者一括変更方法
 Whitelist登録方法
 アラート一覧の取得
 MITRE社 ATT&CKフレームワーク
 Real Time Response機能
 各APIの紹介



運用に活用できる小ネタ集

3

アラートのフィルタリング

networks

	ページ		٢A	Activity] >	٢Det	ecti	ons」	の画	面上部	,)				
	概要		T 川 日 ば ち	ype to 以外の要 1ます。	filter」 素でも	をく 5フィ	7リ、 ルタ	ックす ヌリン	つる事 グす	により る事が	、既に 可能で ⁻	表示さ す。AN	れてい ^に ND条件	る 7 []] で検	項 索
٨		۹ ту	be to filter							671 detections four	nd ×				
()	Activity	Severity Critical High	27 465	TacticExecution336Machine L274	Technique PowerShell 325 Sensor Ba 189	Time Last Lour Last day	0 M 32 I	Status New 64 n Progress	Triggeri 7 powershe 8 explorer.e	ng file Assigne I 329 Unassigne exe 50 igata f@	ed to n 648)ma 18				
	Dashboard Detections Quarantined Files Real Time Response	Medium Low Informat + Q	60 95 ion 24	O X Sei e Actor		Tech	nique	Time		Status	671 of Triggering file	detections found Assigned	to		
	Investigate Host Search Hash Search	Selec	t All	Critic High Meilic Assigned	sion to	336 Powe 274 Sens 135 Spea	rShell 3	25 Last hou	r O oc9dca2f0eabc	New 647 f127b8a77361ac8858	powershel 3 33819923a69502b4e ⁻	29 Unassign ×	648 45 d	detections fou	und X
	User Search Source IP Search Bulk Hash Search		Mec	Lov Infern + C Hash Host Dom	Line Bi	110 Clou 45 Proc more + 익	Severity Critical High Medium	Tac 0 Mac 45 Exe 0 Initi	t ic hine Le 45 sution 44 al Acce 43	Te chnique Se Isor Bas 45 Po verShell 44 Sp arphish 43	Time Last hour () Last day () Last week () Last 30 days 10	Status D New D In Progress D True Positive D False Positive	Triggering file 45 powershell 4 0 Shinobot.e 2 0 shinobot.exe 0 temp.dat	e Assign 44 Unassig 20 17 7	ed to Ined 45
				Se Host First Host ID	Seen		Informatio + Q	onal 0 +Q		+Q	Last 90 days 4	5 Ignored + Q	0 ShinoBOT.exe +Q 2 mo	2 are +Q	
				Host Prod Host Type Hostname	uct Name	CHNIQUE	Select	All §≣ Upde High +2 othe	te & Assign ACTIC & TECHNIQU hitial Access vi	е а S DETECT ТІМЕ 2018-11-06	Ност 16:45:36 VICTIN	prouping ICS A	Soft by time	ASSIGNED Unass	STATUS New
				Objective Operating	System ,			High +3 othe	ACTIC & TECHNIOL NITIAI Access vi	a S ^D DETECT TIME 2018-11-06	ноsт 16:45:32 VICTIN	ICS A	ser NAME Administrator	ASSIGNED _ Unass	New 0
							_	High	ACTIC & TECHNIQU		HOST	u	SER NAME	ASSIGNED	STATUS Q

アラートのグルーピング

networks

ページ	「Activity」 > 「Detections」の画面中部
概要	「No grouping」のタブをクリックすると、ホスト毎・ファイル Hash値・ファイル名毎等のアラートにグルーピング出来ます。
Detections Low Quarantined Files Informa Real Time Response + Q	95 Defense E 110 Cloud Base 74 Last 30 d 202 False Positive 0 Shinobot.e 20 ition 24 Falcon Ove 45 Process Inj 57 Last 90 da 671 Ignored 4 TrustedIns 20 +Q 6 more +Q 19 more +Q +Q 99+ more +Q
 Investigate Host Search User Search Source IP Search Bulk Hash Search Bulk Domain Search Event Search 	Att All I Update & Assign No grouping Sort by newest detect time I Select All I Update & Assign No grouping Sort by newest detect time I Select All I Update & Assign No grouping Sort by newest detect time I Select All I Update & Assign No grouping Sort by newest detect time I Select All I Update & Assign No grouping Sort by newest detect time I Actic & Technique DETECT TIME DETECT TIME No grouping Assigned - status of Unass I Actic & Technique DETECT TIME 2018-12-03 09:45/26 Sort by newest detect of Unass New of O I High TACTIC & TECHNIQUE DETECT TIME DETECT TIME Crouped by Host Grouped by Tactic Grouped by Tactic Grouped by Tactic Grouped by Tactic Grouped by Technique Grouped by Severity Assigned - status of New of O I High TACTIC & TECHNIQUE DETECT TIME DETECT TIME Grouped by Severity I High TACTIC & TECHNIQUE DETECT TIME DETECT TIME Sorte by Technique New of O I High TACTIC & TECHNIQUE DETECT TIME DETECT TIME Coreured by Host New of O
Select All I Update & Assign	Image: High TACTIC & TECHNIQUE Machine Learning DETECT TIME 2018-12-02-00-10-51 Detect TIME 2018-12-02-00-10-51 Strouped by Command line Marking Assigned Stratus Hash値ベース Grouped by Select Update & Assign ホスト名ベース Grouped by Host Sort by newest detect time Sort by newest detect CRITICAL HIGH Medium Low INFO HOSTS CRITICAL HOST LAST SEEN TYPE CRITICAL HIGH Medium Low INFO
HASH	Image: Non-Stand Stand

アラートステータス・担当者一括変更方法

「Activity」 > 「Detections」の画面中部 ページ 個別にステータス・担当者変更も可能ですが、アラートフィルタリン 概要 グやグルーピングを用いて、一括で複数アラートの変更も可能です。 Update selected detection statuses ASSIGN TO SET STATUS CANCEL

macnica networks

Whitelist登録方法



ページ	ΓActiv	ity」 >	[Detect	ions] >	ΓΕΧΕϹυ	ITABLE S	HA256]
概要	Detecti 能です。 Hashes	onsペー 一括で j」ペーシ	ジからの 複数のHa ジからのこ	Whitelist sh値を登録 ご登録がおり	登録の場合 録された 愛めです	合、数クリ い場合は 。	リックで登録可 「Prevention
		Shinobot.ex	e		© []		
		😩 Unassigned	I Co Ne	w (t	Comment		
				O Network Contain			
		🚱 Connect to	Host		Select policy action		×
HELL.EXE		Execution Detai	ls		 Always Block Never Block 		
		DETECT TIME	FIRST BEHAVIOR	MOST RECEN	CA	ANCEL	APPLY
ତ ହାଇ କରୁ	OBOT.EXE ₽	FILE PATH	2018-11-06 16:44 \Device\Harddisk \Documents\Shin	:312018=11-06 :Volume2\Users\Admin :obot.exe	istrator G	fc7cd747364s2c0ce6fs404sf4	4f84a01e26a8932038e5025 i809d33f7
		EXECUTABLE SHA256	262ca19ff3dbc9do 23a69502b4e1bc	ca2f0eabcf127b8a773 703	LIST NAME XHE	意のリスト名を	:記人
			GLOBAL PREVALENCE	LOCAL PREVAL	CA	ANCEL	CONFIRM
			HASH PREVENTION PO		<u>् त्र छि</u>		
		EXECUTABLE MD5	35b9da2067f27ea	ad79872bccb12ebfab			



Whitelistが適用される検知シナリオ

- ┃ 適用対象アラート(OR条件)
 - | 「Tactic」項目が"Machine Learning"となっているアラート
 - 「Technique」項目が"Adware"または"PUP"となっているアラート

※上記シナリオ以外に対するWhitelist登録は弊社までお問い合わせ下さい。

| 適用対象ファイル

| 実行ファイル (exe/dll等) のみ。Microsoft Officeのファイル (.xlsx/.doc等) は登録頂けま せん。

Whitelist化可能要素と登録場所

項目	登録場所
ファイルハッシュ	 Detections > EXECUTABLE SHA256 Configuration > Prevention Hashes
ファイル名	
ファイルパス	③Configuration > File Exclusions
ファイル拡張子	

アラート一覧の取得



ページ	<pre>[Investigate] > [Host Search]</pre>
概要	アラートの一覧を閲覧・取得できます。また、期間を指定してCSVで 出力することも出来ますので、社内用のレポートの基データとしても ご利用頂けます。 「Dashboards」 > 「Detection Activity」からは統計情報を取得頂 けますので、併せてご活用下さい。





MITRE社 ATT&CKフレームワーク

10



- ┃ MITRE(マイター)社について
 - ┃ 脆弱性管理番号(CVE)を発行している米国の非営利研究機関になります。
- ATT&CK(アタック)について
 - **ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge**
 - 大まかな攻撃フェーズを表現した"Cyber Kill Chain"に、<u>具体的な攻撃手法</u>を追加したフレームワークになります。このフレームワークにより、CrowdStrike Falconからの各アラートに対して、<u>攻撃者の目的・攻撃戦術・攻撃手法を理解することができます</u>。

	Cyber Kill Chain (攻手のスノッノ)									
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public- Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Cryptographic Protocol

参考: https://attack.mitre.org/matrices/enterprise/windows/ "© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."



CrowdStrikeでのマッピングについて

| ATT&CKの「Tactic (戦術)」「 Technique (手法)」に加え、 CrowdStrikeは「Objective(目的)」を定義・追加しています。

┃ 「攻撃者は < 目的> を達成するために、 <手法> を使い、 <戦術>を行いまし た。」という理解ができます。

※どの「Objective(目的)」にも該当しない攻撃に関しては、「Falcon Detection Methods 」というObjectiveに分類しています。

Objective	Tactic	Technique	ストーリー解釈
Gain Access	Initial Access	Spearphishing Attachment	攻撃者は <mark>侵入</mark> するために、スピアフィッシング メールを使い、初期侵入を行いました。
Gain Access	Credential Access	Credential Dumping	攻撃者は <mark>侵入</mark> するために、 <mark>認証情報ダンプツー</mark> ルを使い、認証へのアクセスを行いました。
Keep Access	Persistence	Create Account	攻撃者は継続侵入するために、アカウントを作 成し、永続性の確保を行いました。
Keep Access	Defense Evasion	Obfuscated Files or Information	攻撃者は継続侵入するために、ファイルや情報 を難読化し、防御システムの回避を行いました。



▶ 検知画面

- | 検知アイコンの変更
- | アラート通知メールの変更
- API

検知画面

macnica networks

■ これまでの検知シナリオを廃止し、Objective/Tactic/Techniqueへ 表記変更し、説明部分の情報量が増えました。







- これまで検知シナリオ毎にアイコンが用意されていましたが、変更後は Objective毎に用意されています。
- 】さらにブロック時やOverWatch検知時は、アイコンにバッジが付加されるようになりました。

Objective	アイコン	イベント	アイコン
Gain Access		ブロックイベント	S
Keep Access	<->	OverWatchイベント	E
Explore	₽ ₽		
Contact Controlled Systems	R		
Follow Through			
Falcon Detection Methods			

アラート通知メールの変更

macnica networks

【メール本文に検知シナリオが記載されていましたが、「Tactic & Technique」に表記がかわりました。また、ブロックされている場合は 「Severity」項目に"Prevented"と表記されます。



| 2019年1月16日にQuery APIとStreaming APIの一部項目が変更されます。

Query API

変更前の項目名	変更後の項目名
	objective
scenario	tactic
	technique
	pattern_disposition

Streaming API

変更前の項目名	変更後の項目名		
	Objective		
	Tactic		
DetectName	Technique		
	PatternDispositionValue		
	PatternDispositionDescription		



Real Time Response機能

18



Real Time Response(RTR)について

オンラインの Falcon がインストールされた端末に対して、リモー トで用意されたコマンド(ファイルの取得・削除やプロセスのキル等)を実行できるようになります。これまで、対処機能としては端末のネットワーク隔離のみでしたが、本機能の追加により様々な端末追加調査および復旧作業を実行できるため、より洗練されたインシデント対応が可能になります。また、ネットワーク隔離中でも本機能は動作致します。

┃ システム要件

- Powershell : Version 2.0以上
- I.NET Framework : Version 3.5以上
- Falcon Sensor : Version 4.5.6806

| 必要Falcon UIアカウントロール

- Real Time Responder
- ※「Falcon Administrator」に上記ロールは含まれていません。

Real Time Responseの起動



■ 起動方法

- 1. 「Detections」ページから修復を行う端末で発生したアラートを表示、 または「Host Management」から当該端末を検索します。
- 2. [Connect to Host] をクリックします。



実行可能内容

macnica networks

ファイルの内容を表示

画面下部のテキストボックスに実施したいコマンドを入力し、"RUN" をクリックします。取得コマンド(get等)はダウンロードリンクが画面 概要 主要コマンド 上部に表示されます。

cat

Connected to He	ost Name: 11520-DTPC-01 END SESSION	cd	フォルダの移動
C:\> help cat cd	Read a file from disk and display as ASCII or hex Change the current working directory	ср	ファイル・フォルダのコピー
clear cp eventlog	Clear Screen Copy a file or directory Inspect event logs. Subcommands: list, view, export Umbade a file to the Faleon cloud	get	ファイルの取得
getsid help history	Enumerat local users and Security Identifiers (SID) Get help on a specific command or subcommand View History	kill	プロセスの停止
ipconfig kill ls memdump	Show network configuration Kill a process Display the contexts of the specified path Dumb the memory of a process	ls	ファイル一覧表示
mkdir mount mv	Create a new directory List mounted filesystem volumes Move a file or directory	mv	ファイル・フォルダの移動
netstat ps reg rm	Display network statistics and active connections Display process information Windows registry manipulation. Subcommands: query, set, delete, load, unload Remove a file or difectory	ps	プロセス一覧表示
zip C:\>	Compress a file or directory into a zip file	reg	レジストリの検索・登録・削除
	RUN SHOW SUMMARY	rm	ファイル・フォルダの削除
		eventlog	Windowsイベントログ取得
		xmemdump	フルメモリダンプ取得

opyright © 2004-2018 Macnica Networks Corp. All Rights Reserved.	



各 APIの 紹介

macnica networks

■ Falcon APIとして、以下の4つが提供されています。ご利用にあたり、 APIクレデンシャル情報やAPI有効化が必要となりますので、弊社サ ポート窓口までお問い合わせ下さい。

API 名	取得可能情報
Streaming API	 検知イベント Falcon UIの操作イベント
Query API	 カスタムIoC登録 ホスト検索 インディケーターによる検索 検知ステータス設定、変更
Threat Graph API	• プロセス実行などのグラフ可視化
Data Replicator API	 端末からアップロードした端末イベントログ

システム概要

Falcon Data Replicatorを有効化しますと、各ユーザー毎にAmazon S3/SQSのア カウントが用意されます。発行されたアカウント情報とAPIを使い、端末からアップ ロードされたログを自社システムにダウンロードすることができます。

※ダウンロードしたログをCrowdStrike Falconヘリストアする事はできません。



macnica



ご清聴ありがとうございました。 Thank you for your attention.

25