kaspersky

カスペルスキーのインテリジェンスレポートサービスのご紹介

～エキスパートが調査した最新のサイバー攻撃に関する情報を提供～

V1.1

2023年06月23日

株式会社カスペルスキー
セールスエンジニアリング本部

Kasperskyが提供するレポートサービス

注目度の高いサイバースパイ活動に関するタイムリーな情報を提供

・カスペルスキーのエキスパートが調査した最新のサイバー攻撃に関する非公開レポートを提供するサービス。

・攻撃および業界に特化した以下3種類のレポートを提供
 -**APT Intelligence Reporting:** APT・標的型攻撃に関する情報
 -**Crimeware Intelligence Reporting:** 金銭目的のサイバー犯罪に関する情報
 -**ICS Threat Intelligence Reporting:** 産業組織を標的とするサイバー犯罪に関する情報

・過去に発行されたすべてのレポートはカスペルスキーの脅威インテリジェンスポータルサイト:
「Kaspersky Threat Intelligence Portal」からダウンロード可能。

・技術的詳細を記述したフルレポート、C-レベルに向けたExecutive Summary の2種類を用意。

・レポートだけでなく脅威検知に使用出来る IOC、YARAを提供。

・ TAGによるフィルタリング(産業、国などをフィルタリング)

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting とは

APT Intelligence Reportingの特徴

- グローバル調査分析チーム「GReAT」が現在調査中の最先端の脅威に関するレポート
  - ✓ 一般には公開されない攻撃事案に対するレポート
  - ✓ 調査の進捗、攻撃者グループの戦術や技術の変化に応じたレポートのアップデートとメールによるアラート
  - ✓ 地域毎・業種毎・攻撃者グループ毎の検索タグと全文検索

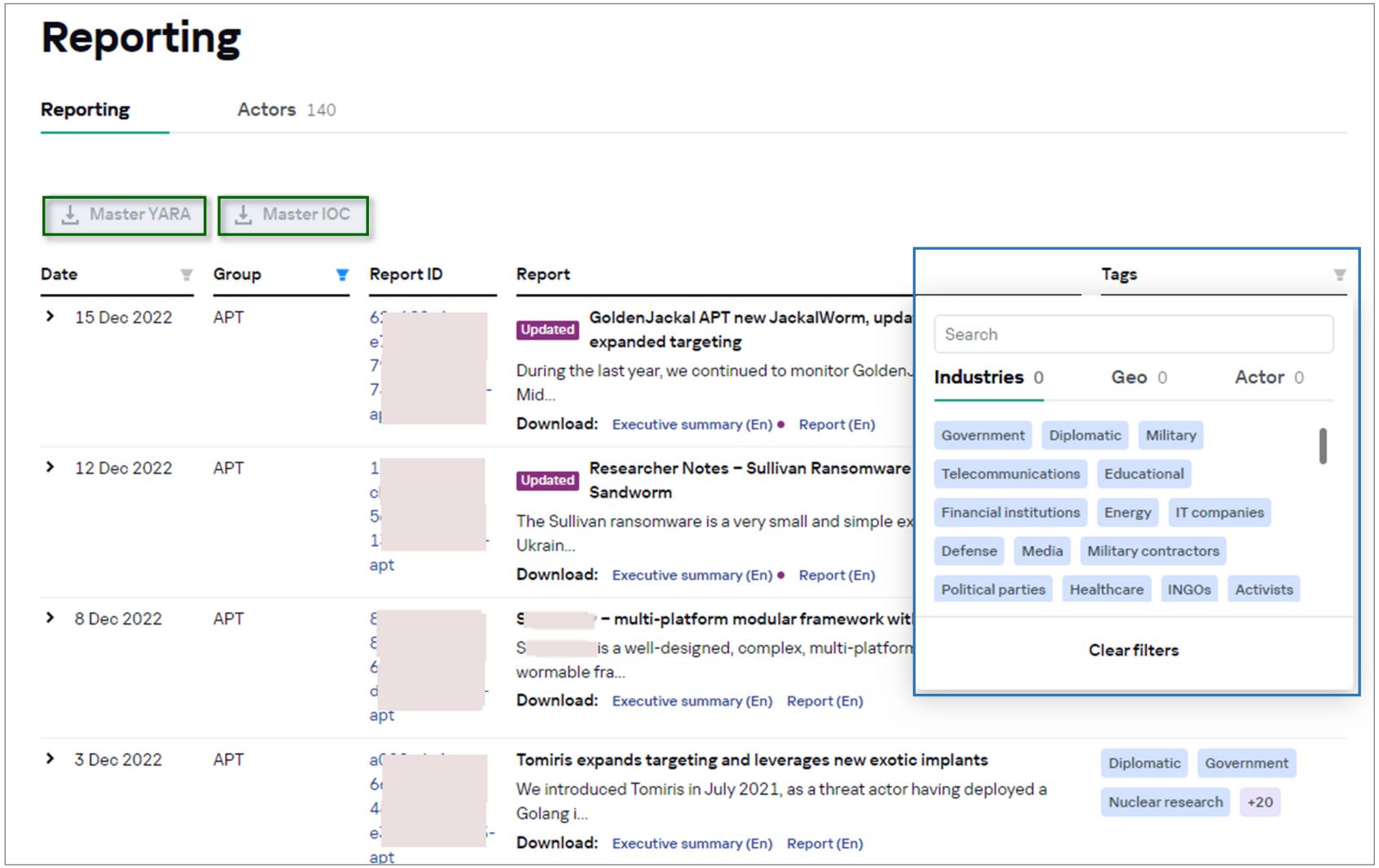
- 経営層や管理職からセキュリティ専門技術者までを対象とした読みやすく実戦的なレポート内容
  - ✓ 攻撃の概要（Executive Summary）
  - ✓ 技術的詳細（Technical Details）
  - ✓ 攻撃の戦術、技術および手法（TTPs）とMITRE ATT&CKマッピング
  - ✓ 攻撃者の属性情報（Attribution）

- 脅威ハンティングに使用できる機械読取可能なIoCを提供（openIOC、YARA）

- 脅威アクター（攻撃者グループ）のプロファイル情報

Copyright © 2023 Kaspersky Lab. All rights reserved.

TAGによるフィルタリング



Copyright © 2023 Kaspersky Lab. All rights reserved.

Building a safer world

カスペルスキーのグローバル調査分析チーム「GReAT」による取り組み

・40人を超えるGReATのメンバーは、ヨーロッパ・ロシア・アメリカ・アジア・中東ほか世界各地で業務にあたり、世界中のサイバー攻撃に関する動向を調査・分析しています。

GReATが調査・公表してきたAPT攻撃に使用された言語

英語： Regin, Equation, Duqu2.0, Lamberts, ProjestSauron

ロシア語： Moonlight Maze, RedOctober, CloudAtlas, Miniduke, CosmicDuke, Epic Turla, Penquin Turla, Turla, Black Energy, Agent.BTZ, TeamSpy,

中国語： Icefog, SabPub, Nettraveler, Spring Dragon, Blue Termite

韓国語： Darkhotel, Kimsuky, Lazarus

アラビア語： Desert Falcons, Stonedrill, Shamoon

スペイン語： Careto/Mask, El Machete

フランス語： Animal Farm

GReATが活動を追跡する主な脅威アクター

2016	2017	2018	2019	2020	2021
ProjectSauron	WannaCry	Zebrocy	Topinambour	Cycldek	GhostEmperor
StrongPity	Shamoon 2.0	DarkTequila	ShadowHammer	SixLittleMonkeys (aka Microcin)	ExCone
Lazarus	StoneDrill	MuddyWater	SneakyPastes	CactusPete	BlackShadow
Fruity Armor	BlueNoroff	Skygofree	FinSpy	DeathStalker	BountyGlad
ScarCruft	ExPetr/NotPetya	Olympic Destroyer	DarkUniverse	MATA	EdwardsPhesant
Poseidon	Moonlight Maze	ZooPark	COMpfun	TransparentTribe	HotCousin
Danti	ShadowPad	Hades	Titanium	WellMess	GoldenJackal
Dropping Elephant	BlackOasis	Octopus		TwoSail Junk	FerociousKitten
	Silence	AppleJeus		MontysThree	ReconHellcat
	WhiteBear			MosaicRegressor	CoughingDown
				VHD Ransomware	MysterySnail
				WildPressure	CraneLand
				PhantomLance	

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

Executive Summary : C-レベル（意思決定者）向けレポート

・経営層・リーダーがセキュリティに関する適切な意思決定・投資判断のインプットとして活用できるように、攻撃の概要を要約したレポートを提供します。

TLP: AMBER

kaspersky

BlueNoroff employs new tools in recent activity

Report Id: 20190802
Version: 1.0 (5.August.2019)

Executive Summary

We recently tracked new BlueNoroff activity following the previously reported[12] campaigns. In particular, we found an bank in Myanmar compromised by this actor. We promptly contacted them, sharing the IOCs we had found.

This collaboration allowed us to learn valuable information on how they move laterally to access high valuable hosts, such as ones owned by the bank´s system engineers interacting with SWIFT. They used a public login credential dumper and homemade Powershell scripts for lateral movement.

BlueNoroff also starts to employ new malware with an uncommon structure, probably to slow down its analysis. Depending on the command line parameters, this malware can run as passive backdoor, active backdoor and tunneling tool. We assess that the actor runs this tool in different modes depending on the situation.

Moreover, we found another type of Powershell script used by this group when they attacked a victim in Turkey. This Powershell has similar functionalities with the ones previously used, but

This report in a nutshell:

- The actor utilized a Google Docs look-alike app, hosted on PaaS platforms for initial compromise;
- The open-source 'Ares RAT' was used as a payload in the attacks;
- The waves of attacks have been ongoing for more than a year, and most likely are originating from

Techniques, Tactics and Procedures specific for this campaign:

Infrastructure

Link shorteners; Cloud storage; VPS

Infection vector

Spear phishing emails with attachments; Spear phishing emails with urls redirecting to fake Google Docs apps

Implants

Copyright © 2023 Kaspersky Lab. All rights reserved.

kaspersky

APT Intelligence Reporting：レポートサンプル

Full Report：SOC担当者、セキュリティ専門技術者向けレポート

①技術的詳細
例：　-攻撃の背景、ペイロードをダウンロードさせるために攻撃者が使用する手法やツール
　　-検知回避するための難読化の手法、ペイロード実行後に行われるバックドア設置などの永続化の手法

Technical Details

Initial Infection

The campaigns discussed in this report began with spear phishing emails. While many of the initial emails were not obtainable by us, using our statistical data and telemetry we were able to reconstruct what we believe is the entire infection chain. Moreover, the actor's heavy usage of public services such as URL shorteners allowed us to get a broad view of their operational activity. We divide this activity into two different campaigns based on how the initial access was obtained. The first campaign began in December 2017 and was completed around August 2018, while the second one began around October 2018 and still goes on.

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]
B0lad
Owner: [redacted]@gmail.com
Filename: Wedding Invitation.pdf
Created Time: 2018-01-08 06:58:34
Modified Time: 2018-01-0806:58:42
MD5: 3919a78[redacted]c44cb5ab

Data Exfiltration

The purpose of the attacks appears to be pure data theft. Sometimes after a successful compromise, the malware will receive the following set of commands:

- List current catalogue with `dir`
- Download "o.txt" from the C2 (i.e. - http://[redacted]/static/x/o.txt)
- Rename "o.txt" to "o.bat" and execute it

The code contained in o.txt[6] will then download the following additional files from Dropbox.

Original EXE Name	Name of Downloaded EXE	Hash
7za.exe[7]	tmp.exe	5E0CFB5F[redacted]C9B1
rclone.exe[8]	system.exe	59B363E5[redacted]6ED8
rclone.conf	rclone.conf	F68D250C[redacted]AF8E

Next, it will look for all files with the following file types on the victim's file system:

- Documents - files with extension .doc, .docx, .odt, .pdf
- Spreadsheets - files with extension .xls, .xls, .ots
- Presentations - files with extension .ppt, .ppsx, .pptx, .odp

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

Full Report：SOC担当者、セキュリティ専門技術者向けレポート

②攻撃に使用されるインフラストラクチャ
-APT攻撃に利用されるC＆Cサーバーやパブリックサービス、Webサイト

Infrastructure

Fishing Elephant operators heavily rely on URL shortening services and cloud storage services for the first stage in the infection chain. Below is a list of shortened URLs observed in these campaigns.

Short URL	Final URL	# of Clicks	Creation Time
http://bit[redacted]	https://[redacted]NgbifyA	122	03-10-2018 11:00:21
http://bit[redacted]	https://[redacted]3GHpgg	10	18-01-2019 06:37:40
http://bit[redacted]	https://[redacted]z31LQ	21	18-01-2019 06:39:55
http://bit[redacted]	https://[redacted]3YfoEv	6	02-07-2018 10:46:52
https://go[redacted]	https:/[redacted]Z3QnSCw	7	20-12-2017 10:38:58
https://go[redacted]	https://[redacted]3RBhG6	42	04-01-2018 07:19:06
https://go[redacted]	https://[redacted]3RBh4y	61	04-01-2018 07:17:47
http://bit[redacted]	https://[redacted]3Yk3pV	5	04-07-2018 06:08:46
http://bit[redacted]	https://[redacted]3XjzmH	8	11-06-2018 08:09:28
http://bit[redacted]	https://[redacted]3ViKqf	5	11-05-2018 09:47:47
http://bit[redacted]	https://[redacted] navigate[redacted] 442118D02844	63	02-07-2018 07:00:26
http://bit[redacted]	https://[redacted] navigate[redacted] CA95089D06E4	34	11-06-2018 05:20:22

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

Full Report：SOC担当者、セキュリティ専門技術者向けレポート

③APT攻撃の被害が確認された地域

Victims

The main target vertical for [redacted] appears to be high profile political and military targets in South Asia, specifically countries bordering [redacted]. Below is a geographic distribution of potential victims we observed based on our statistical data.

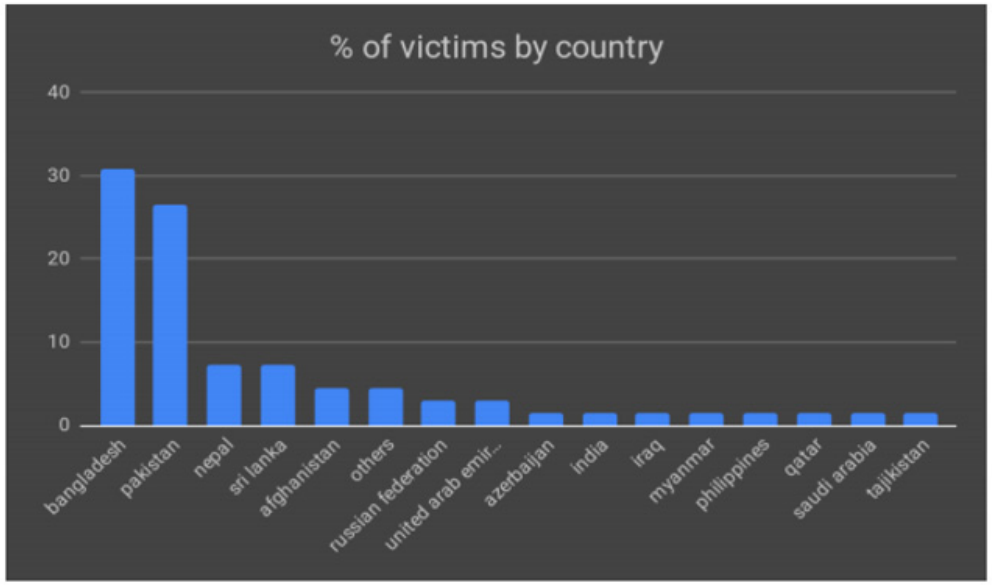


Fig. 4 Distribution of targeted countries

Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

Full Report：SOC担当者、セキュリティ専門技術者向けレポート

④IoC、YARAルール（機械読取可能な形式でも提供）
-調査・分析によって確認されたIoC
-グローバル調査分析チームが調査で使用したYARAルール

Appendix I – Indicators of Compromise

Note: *The indicators in this section are valid at the time of publication. Any future changes will be directly updated in the corresponding .ioc file.*

File Hashes

DDE Word Documents

0817771[redacted]E870
1289358[redacted]3833
2EE8075[redacted]3B08
49AAC64[redacted]F761
652D716[redacted]92CC
A404E51[redacted]2431
AF62E77[redacted]518A

VBS Scripts

007491D[redacted]156B
7648C5F[redacted]3028
2F079E9[redacted]FE2A
0882DCA[redacted]9102
0245B26[redacted]6CB0
681CF84[redacted]33A8
A085CD6[redacted]E0CC
F945C0E[redacted]68CE
41388D3[redacted]AE26
65ACFB9[redacted]86EA
05CDF28[redacted]D7DA
DBA85C8[redacted]F7AD
6F0E866[redacted]C939
95BD3ED[redacted]355E
90816A8[redacted]D380

Yara

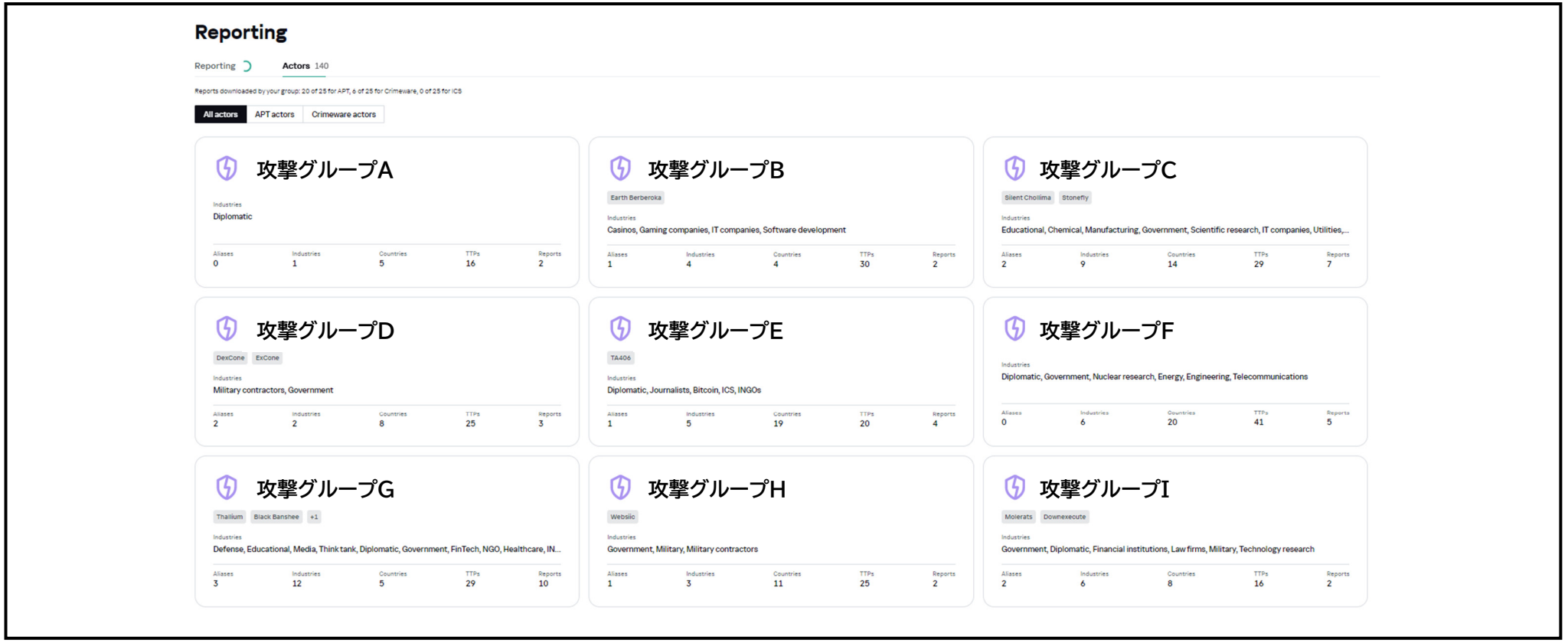
```
rule apt_[redacted]ddedoc{

    meta:
        copyright = "Kaspersky Lab"
        date = "2019-04-18"
        description = "Detects DDE payload using bitsadmin to download hta"

    strings:
        $a0 = "QUOTE"
        $a1 = [redacted]
        $a2 = [redacted]
        $a3 = [redacted]
        $a4 = "101 114 32 100 97 116 97 32 47 112 114 105 111 114 105 116 121 32
104 105 103 104 32"
        $a5 = "word/document.xmlP"
        $a6 = "REF c"
        $a7 = "REF d"
        $a8 = "REF e"
        $a9 = "104 116 116 112"

    condition:
        all of them
}
```


Copyright © 2023 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：プロファイル情報

攻撃グループに関する情報、レポートを確認

・攻撃グループがターゲットとする地域、主な攻撃手法およびマルウェア、MITRE ATT&CKマトリクス、関連する発行済みレポートなどが確認可能なプロファイル情報をポータルサイトから閲覧可能です。



Copyright © 2023 Kaspersky Lab. All rights reserved.

Crimeware Intelligence Reporting

Copyright © 2023 Kaspersky Lab. All rights reserved.

Crimeware Intelligence Reporting とは

Crimeware Intelligence Reportingの特徴

- <u>さまざまなセクターを標的とする金銭目的のサイバー犯罪に関するレポート</u>
  - ✓ 対象：主に金融機関とその大口顧客、対応する政府機関、および M&A 取引に関与する企業
  - ✓ 特定のインフラストラクチャ（ATM や POS デバイスなど）に対する攻撃情報
  - ✓ 広範で危険なマルウェアキャンペーン
  - ✓ さまざまな地域のダークウェブマーケット上でサイバー犯罪者によって使用、開発、または販売されている特定のクライムウェアツールに関する情報

- <u>レポート、IoC、YARAに加え、Sigmaルールを提供</u>

  ※ Sigmaルールとは：
  ログファイルに対する汎用的なシグネチャフォーマットで、SIEMを使用した脅威を検知するためのルールを定義。
  SigmaをサポートするSplunk、Elastice Searchなどの製品、MISPなどのOSSなど各SIEMのクエリに変換可能なため、
  SIEMに依存することなくルールを適用可能。

- <u>脅威アクター（攻撃者グループ）のプロファイル情報</u>

Copyright © 2023 Kaspersky Lab. All rights reserved.

ICS Threat Intelligence Reporting

Copyright © 2023 Kaspersky Lab. All rights reserved.

ICS Threat Intelligence Reporting とは

ICS Threat Intelligence Reportingの特徴

- 産業制御システム(ICS)に関連するサイバー脅威に関するレポート
  - ✓ 産業組織を標的とした新たなAPT、攻撃キャンペーンおよび活発な脅威に関する最新情報
  - ✓ SCADA、PLC、リモート管理ツールなどICS関連の脆弱性情報の提供
  - ✓ 脆弱性がどのように悪用されるのかといった内容や、リスク緩和のための推奨アクションも提供

- 直近1ヵ月に発生した産業組織をターゲットにした攻撃の概要をまとめたマンスリーレポート
  - ✓ 産業組織をターゲットにした攻撃のトレンド、流行する地域の把握に活用
  - ✓ 地域ごとの統計情報

    <レポートで提供する統計情報>

    -脅威の発生源(インターネット、Email、リムーバブルデバイスなど)

    -脅威タイプ(スクリプト、悪意のあるドキュメント、トロイの木馬など)

    -分野(製造業、オイル・ガス、電力・エネルギーなど)ごとの攻撃の被害状況の詳細

Copyright © 2023 Kaspersky Lab. All rights reserved.

ライセンス

Copyright © 2023 Kaspersky Lab. All rights reserved.

ライセンス

年間ライセンスとバンドルライセンスの2種類を提供

①年間ライセンス

・APT Intelligence ReportingとCrimeware Intelligence Reportingの場合、以下のレポートが購読可能

<年間ライセンスに含まれるレポート・ファイル>

-Executive Summary + Full Report

-機械読取可能な形式のIoCファイル・YARAルール

・ ICS Threat Intelligence Reportingの場合、以下2つのパターンから選択可能

1. Full Report & Executive Summary and IoCs

<このライセンスに含まれるレポート・ファイル>

-Executive Summary + Full Report: セキュリティ専門技術者向けレポート

-機械読取可能な形式のIoCファイル・YARAルール・Suricataルール

2. Executive Summary and IoCs

<このライセンスに含まれるレポート・ファイル>

-Executive Summary

-機械読取可能な形式のIoCファイル・YARAルール・Suricataルール

※Executive Summary: 経営層(意思決定者)向けレポート / Full Report: セキュリティ専門技術者向けレポート

Copyright © 2023 Kaspersky Lab. All rights reserved.

ライセンス

年間ライセンスとバンドルライセンスの2種類を提供

②バンドルライセンス
・以下2種類のバンドルライセンスから選択可能

1. APT + Crimeware
<このバンドルライセンスに含まれるレポート・ファイル>
-Executive Summary: APT + Crimeware
-Full Report: APT + Crimeware
-機械読取可能な形式のIoCファイル・YARAルール: APT + Crimeware

2. APT + Crimeware + ICS
<このライセンスに含まれるレポート・ファイル>
-Executive Summary: APT + Crimeware + ICS
-Full Report: APT + Crimeware
-機械読取可能な形式のIoCファイル・YARAルール: APT + Crimeware + ICS

Copyright © 2023 Kaspersky Lab. All rights reserved.
kaspersky

kaspersky