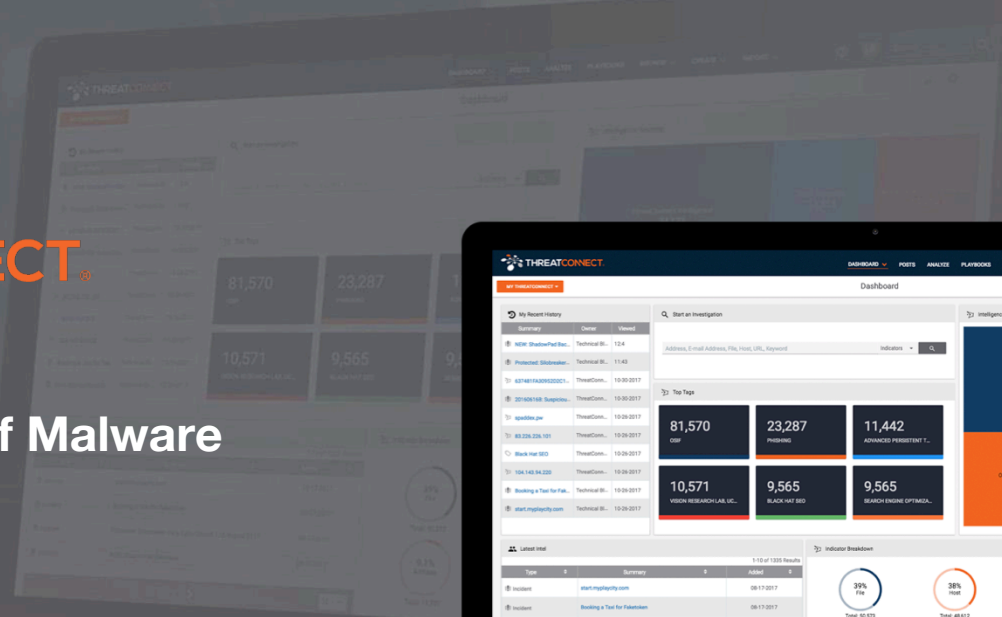




Cloudy with a Chance of Malware

Marika Chauvin
Senior Threat Intelligence Researcher
ThreatConnect



About Me



- Senior Threat Intelligence Researcher at ThreatConnect
- Graduate of Southern Miss and American University
- Borderline obsessed with Harry Potter (Ravenclaw FTW!)
- Dog instagram



Laissez les bon temps rouler



Table of Contents



Introduction

- KASPERAGENT vs Cloudy

KASPERAGENT

- Background
- OPAERA

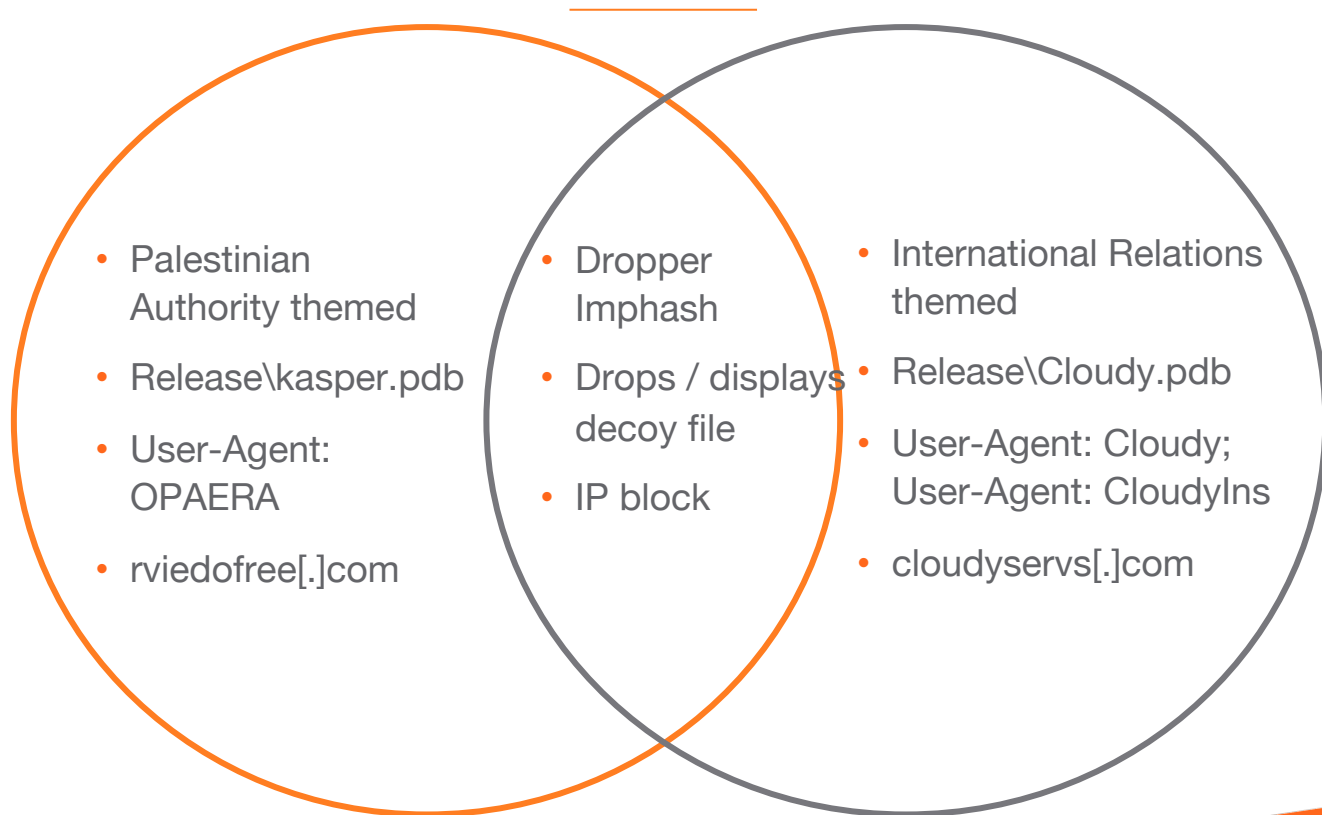
Cloudy

- YARA hunting
- Overlaps

Conclusions

- Targets
- Attribution
- Next steps

KASPERAGENT vs Cloudy



Background

KASPERAGENT and Micropsia

- Links to Android malware
- Publicized in 2017

Middle East-based threat

Known targets:

- US
- Israel
- Palestinian Territories
- Egypt



© 2018 ThreatConnect, Inc. All Rights Reserved.



Phantom of the Opaera

- May 2017
- KASPERAGENT campaign
- OPAERA user-agent string
- mailsinfo[.]net
- windowsnewupdates[.]com
- Palestinian Authority-themed
- Possible Palestinian Authority targets



التاريخ 2017/4/10م

سري جداً ..

الاخ / يحيى المنوار.. "ابو ابراهيم" حفلة الله
السلام عليكم ورحمة الله وبركاته ...

الموضوع / بشأن لجنة التحقيق في قضية اغتيال الشهيد القائد مازن فقها

- بناء على الصلاحيات المخولة لنا بشأن لجنة التحقيق في قضية اغتيال الشهيد القائد مازن فقها التي تم تشكيلها بتاريخ 24/3/2017م، فقد تم اغلاق ملف التحقيق بشكل كامل بناء على طلبكم وتسليم جميع الادلة ومتعلقات القضية للاخوة في الأمن طرفكم من تاريخه.

العهد ساسي عودة
مدير عام جهاز الأمن الداخلي

المحرر مواننا جبرية الرضبة
أف كن
أبراهيم

YARA Hunting: KASPERAGENT Dropper

Simple rule

Imphash

PDB string

```
rule KASPERAGENT_Dropper
{
  strings:
    $str1 = "\\Merge\\Release\\testproj.pdb"
  condition:
    any of them or imphash contains "2bceb64cf37acd34bc33b38f2cddfb61"
}
```



Notified based on YARA rule
New samples looked different

-

8

THREATCONNECT

DASHBOARD ▾ POSTS ANALYZE PLAYBOOKS BROWSE ▾ SPACES ▾ CREATE ▾ IMPORT ▾ MCHALVIN ▾ ⓘ PK Search

FILTERS ▾ Contains Text Clear All Advanced ✕

Attributes Import Hash = 2ba0e6fcf7acd94bc33bf2c6df81 ✕

Type ▾	Summary ▾	Owner ▾	Threat Rating ▾	ThreatAssess ▾	Obs ▾	F/P ▾	Tags	Added ▾	Modified ▾
File	12F9B161AF36B000EEDE0E834BAF0 : 40713DF32EE4F7190380E194149...	ThreatConnect Resear...	🔴🔴🔴🔴	850	-	-	Dropper Kaspersant	09-28-2017	05-31-2018
File	9A05A88E22220B30C587CD0CF2DFFEF3F : 191D9185AC4E168A256F6F870...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-02-2017	05-31-2018
File	C0A353DEA66AB8A57761DC8240DC91D : D263193052CB7A257393C272F...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	10-02-2017	05-31-2018
File	107F10FC002743E34BF4A925BCAE8A1 : E8751A943AD1ED0F8F782B7118...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	10-03-2017	05-31-2018
File	A68F445CF247AD4E07DD06FE1CB9C021 : 0EC741DCF9FC22058098EFC0C...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	10-02-2017	05-31-2018
File	2488473905926B93697538110D2360029 : 4D2986447D6874071BE39A3F7...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	08-31-2017	05-31-2018
File	24D42DAF8C9974711EE3FE024BA6ECA : 10FA03FB0603C48561F0580232...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	08-31-2017	05-31-2018
File	BF829CF99682602850ADA0E30A1E346 : DA482AE950C02A11EEACC210C...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	08-22-2017	05-31-2018
File	996F2131D6675D2691EA3DB1AD0BCA9E : DA7AC703DF2F1AC03FA26804C...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	08-31-2017	05-31-2018
File	C944BFA03579C60919F79781BEA81A : CA66C3526C3CB7921EE8F33C...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	10-03-2017	05-31-2018
File	D192568864815A09A80B3C5E6B48AE : FASD56483AD5367019158E71A...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Cloudy	10-04-2017	05-31-2018
File	4E41BE8630405E9921B0814C17238F : DEDE9E97D31165920C79F7CA7A...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-23-2017	05-31-2018
File	BEB743CB2A7FA032C6A0E07F41BE34F7 : B05006DE2B091AAE2E5E12A7B...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-24-2017	05-31-2018
File	CC2D20250962561A686F82224CA388 : 1233371ED456387233FE97FA39...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-25-2017	05-31-2018
File	A28DD09EFC0A5CE18320B9H4GD47F1 : AA418E8152EB4FBB4274069E...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-25-2017	05-31-2018
File	48B001877C3A9F9610D04A68851A4 : 403DE12C06C0ADB79B9482B...	ThreatConnect Resear...	🔴🔴🔴	850	-	-	Dropper Kaspersant	10-02-2017	05-31-2018

1-35 of 35 Results

Cloudy Dropper, too?

Similar to KASPERAGENT
Dropped Cloudy instead
Callouts triggered rules:

- Arid Viper
- APT-C-23
- Desert Falcons

International relations-themed





Potential connections


Overlaps

newimage3[1].jpg

Download Disabled


Hash Seen Before


Size 631B (631 bytes)

Type 

Description JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 8x9, frames 3

Runtime Process WINWORD.EXE (PID: 3844)

MD5 5aa25a3390662f68ac473d2ebc51697e 

SHA1 eb87971a57a8f11133c127a2dd2431df979985fa 

SHA256 9dcd3b91ed533d7ce9af0b4d21a7842ad33bdf426f82c8878c998ed13bb582b 

- KASPERAGENT decoy
- cloudyservs[.]com

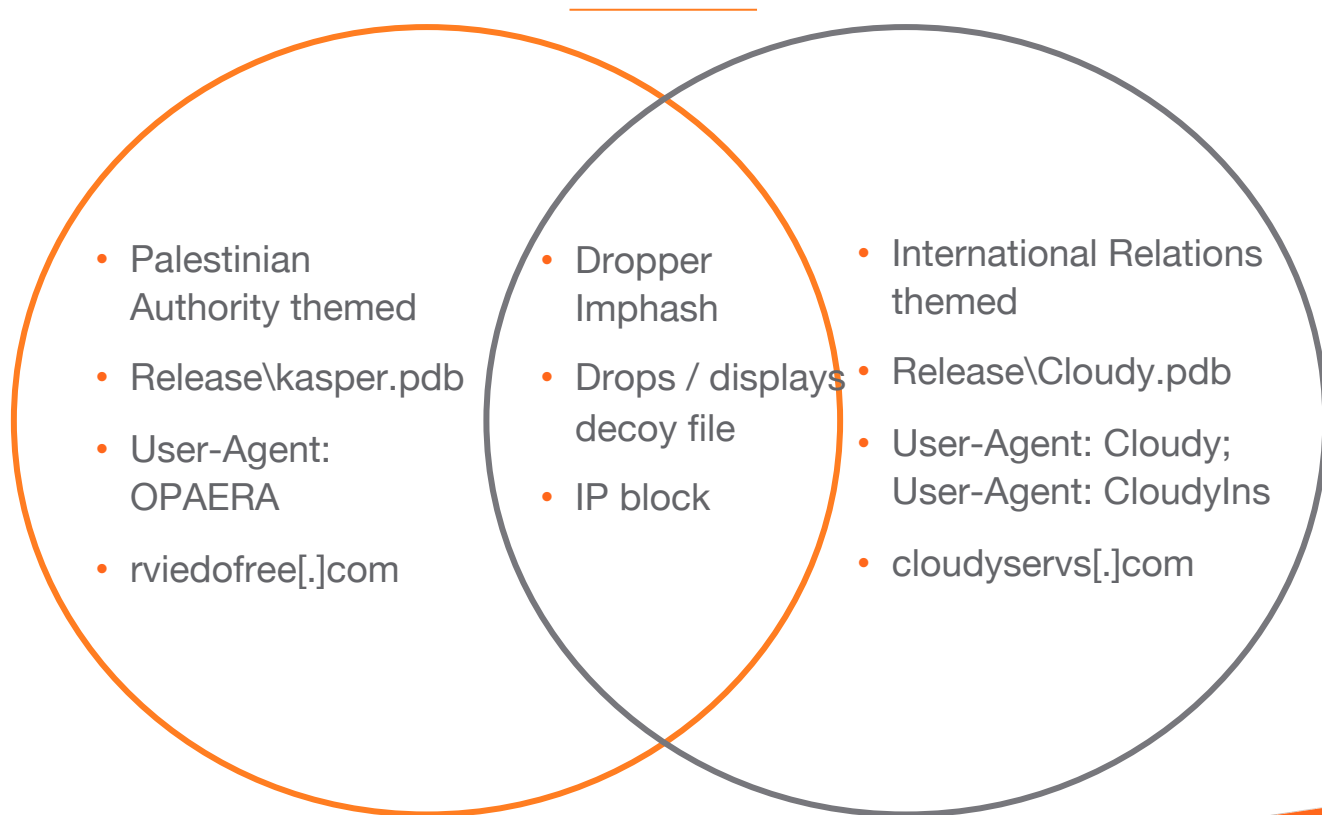
This file has been spotted as the response content of the following URLs.

.....
<http://cloudyservs.com/pic/pic1.jpg>
.....

<http://www.stikerscloud.com/newimages/newimage1.jpg>



KASPERAGENT vs Cloudy



Conclusions



Possible Targets

Submitter countries

Some outliers

Decoy document
themes

KASPERAGENT

Palestinian Territories

Israel

United States

Cloudy

Palestinian Territories

Israel

India

Philippines

United Arab Emirates



- Unconfirmed
- Likely Middle East-based
- Interested in both Israel and Palestinian Authority
- Perhaps a non-state entity

- Unconfirmed
- Likely Middle East-based
- Interested in both Israel and Palestinian Authority
- Perhaps a non-state entity



YARA Hunting: Specific Variants

```
rule KASPERAGENT
{
  strings:
    $a1 = "\\Release\\kasper.pdb"
    $a2 = "\\Release\\testproj.pdb"
  condition:
    all of them
}

rule KASPERAGENTUserAgent
{
  strings:
    $ua1 = "User-Agent: OPAERA"
    $str1 = "addCity.php"
    $str2 = "town.php"
    $str3 = "sign.php"
    $str4 = "getreoponseIndividule.php"
    $str5 = "theRoadSlected.php"
    $str6 = "backapps//backup15"
    $str7 = "city//ammount.php"
    $str8 = "backup15"
    $str9 = "ammount.php"
  condition:
    all of ($ua*) and 1 of ($str*)
}
```

```
rule CLOUDY_PDBString
{
  strings:
    $str1 = "\\Release\\Cloudy.pdb"
    $str2 = "\\Release\\testproj.pdb"
  condition:
    all of them
}

rule CLOUDYUserAgent
{
  strings:
    $ua1 = "User-Agent: Cloudy"
    $ua2 = "User-Agent: CloudyIns"
    $ua3 = "User-Agent: "
    $str1 = "add_virtual.php"
    $str2 = "add_one.php"
    $str3 = "check_ins.php"
    $str4 = "time.php"
    $str5 = "get_tok.php"
    $str6 = "check_st.php"
  condition:
    all of ($str*) and 1 of ($ua*)
}
```





THREATCONNECT®

Thank You

Twitter: @MarSChauvin

Instagram: @KingsleyDoodlebolt

www.ThreatConnect.com