

June 14, 2017

Phantom of the Opera: New KASPERAGENT Malware Campaign

In [Blog](#), [Featured Article](#), [Threat Research](#)

KASPERAGENT Malware Campaign resurfaces in the run up to May Palestinian Authority Elections

ThreatConnect has identified a KASPERAGENT malware campaign leveraging decoy Palestinian Authority documents. The samples date from April - May 2017, coinciding with the run up to the May 2017 Palestinian Authority elections. Although we do not know who is behind the campaign, the decoy documents' content focuses on timely political issues in Gaza and the IP address hosting the campaign's command and control node hosts several other domains with Gaza registrants.

In this blog post we will detail our analysis of the malware and associated indicators, look closely at the decoy files, and leverage available information to make an educated guess on the possible intended target. Associated indicators and screenshots of the decoy documents are all available [here](#)

[\[https://app.threatconnect.com/auth/campaign/campaign.xhtml?campaign=4219181\]](https://app.threatconnect.com/auth/campaign/campaign.xhtml?campaign=4219181) in the ThreatConnect platform.

Some of the indicators in the following post were published on AlienVault OTX on 6/13.

Background on KASPERAGENT

KASPERAGENT is Microsoft Windows malware used in efforts targeting users in the United States, Israel, Palestinian Territories, and Egypt since July 2015. The malware was discovered by Palo Alto Networks Unit 42 and ClearSky Cyber Security, and publicized in April 2017 in the Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA [\[https://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/\]](https://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/) blog. It is called KASPERAGENT based on PDB strings identified in the malware such as "c:\Users\USA\Documents\Visual Studio 2008\Projects\New folder (2)\kasper\Release\kasper.pdb."

The threat actors used shortened URLs in spear phishing messages and fake news websites to direct targets to download KASPERAGENT. Upon execution, KASPERAGENT drops the payload and a decoy document that displays Arabic names and ID numbers. The malware establishes persistence and sends HTTP requests to the command and control domain mailsinfo[.]net. Of note, the callbacks were to PHP scripts that included /dad5/ in the URLs. Most samples of the malware reportedly function as a basic reconnaissance tool and downloader. However, some of the recently identified files display "extended-capability" including the functionality to steal passwords, take screenshots, log keystrokes, and steal files. These "extended-capability" samples called out to an additional command and control domain, stickerscloud[.]com. Additionally, early variants of KASPERAGENT used "Chrome" as the user agent, while more recent samples use "OPAERA" - a possible misspelling of the "Opera" - browser. The indicators

associated with the blog article are available in the ThreatConnect Technical Blogs and Reports source [here](https://app.threatconnect.com/auth/incident/incident.xhtml?incident=4003314) [<https://app.threatconnect.com/auth/incident/incident.xhtml?incident=4003314>].

The samples we identified leverage the same user agent string “[OPAERA](https://app.threatconnect.com/auth/indicators/details/customIndicator.xhtml?id=29927402&owner=Common+Community) [<https://app.threatconnect.com/auth/indicators/details/customIndicator.xhtml?id=29927402&owner=Common+Community>]”, included the kasper PDB string reported by Unit 42, and used similar POST and GET requests. The command and control domains were different, and these samples used unique decoy documents to target their victims.

Identifying another KASPERAGENT campaign

We didn’t start out looking for KASPERAGENT, but a file hit on one of our YARA rules for an executable designed to display a fake XLS icon - one way adversaries attempt to trick targets into thinking a malicious file is innocuous. The first malicious sample we identified ([6843AE9EAC03F69DF301D024BFDEFC88](https://app.threatconnect.com/auth/indicators/details/file.xhtml?file=6843AE9EAC03F69DF301D024BFDEFC88) [<https://app.threatconnect.com/auth/indicators/details/file.xhtml?file=6843AE9EAC03F69DF301D024BFDEFC88>]) had the file name “testproj.exe” and was identified within an archive file ([4FE7561F63A71CA73C26CB95B28EAE8](https://app.threatconnect.com/auth/indicators/details/file.xhtml?file=4FE7561F63A71CA73C26CB95B28EAE8) [<https://app.threatconnect.com/auth/indicators/details/file.xhtml?file=4FE7561F63A71CA73C26CB95B28EAE8>]) with the name “التفاصيل الكاملة لأغتيال فقهاء r24”. This translates to “The Complete Details of Fuqaha's Assassination”, a reference to Hamas military leader Mazen Fuqaha [who was assassinated](https://www.nytimes.com/2017/03/27/world/middleeast/mazen-fuqaha-hamas-killing-israel.html) [<https://www.nytimes.com/2017/03/27/world/middleeast/mazen-fuqaha-hamas-killing-israel.html>] on March 24, 2017.

We detonated the file in [VxStream’s automated malware analysis capability](https://www.hybrid-) [

[analysis.com/sample/16df435ea8214cb0a62ab40720d8d0f5b65ba9268c84fc9e](https://www.hybrid-analysis.com/sample/16df435ea8214cb0a62ab40720d8d0f5b65ba9268c84fc9e) and found testproj.exe dropped a benign Microsoft Word document that pulls a jpg file from [treestower\[.\]com](https://app.threatconnect.com/auth/indicators/details/host.xhtml?host=www.treestower.com&owner=Common+Community) [<https://app.threatconnect.com/auth/indicators/details/host.xhtml?host=www.treestower.com&owner=Common+Community>]. Malwr.com observed this site in association with another sample that called out to mailsinfo[.]net - a host identified in the [Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA](http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/) [<http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/>] blog. That was our first hint that we were looking at KASPERAGENT.

The jpg pulled from [treestower\[.\]com](https://app.threatconnect.com/auth/indicators/details/host.xhtml?host=www.treestower.com&owner=Common+Community) displays a graphic picture of a dead man, which also appeared on a Palestinian news website discussing the death of Hamas military leader Mazen Fuqaha. A separate malicious executable - [2DE25306A58D8A5B6CBE8D5E2FC5F3C5](https://www.hybrid-analysis.com/sample/5d329690a606857871f007b990b78f876c57a571b38cafd!environmentId=100) [<https://www.hybrid-analysis.com/sample/5d329690a606857871f007b990b78f876c57a571b38cafd!environmentId=100>] (vlc.exe) - runs when the photograph is displayed, using the YouTube icon and calling out to several URLs on [windowsnewupdates\[.\]com](https://app.threatconnect.com/auth/indicators/details/host.xhtml?host=windowsnewupdates.com&owner=Common+Community) [<https://app.threatconnect.com/auth/indicators/details/host.xhtml?host=windowsnewupdates.com&owner=Common+Community>]. This host was registered in late March and appears to be unique to this campaign.

With our interest piqued, we pivoted on the import hashes (also known as an imphash), which captures the import table of a given file. Shared import hashes across multiple files would likely identify files that are part of the same malware family. We found nine additional samples sharing the imphash values for the two executables, [C66F88D2D76D79210D568D7AD7896B45](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2) [[https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20\(%22Address%22%2C%20%22EmailAddress%22%2](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

and DCF3AA484253068D8833C7C5B019B07

[[https://app.threatconnect.com/auth/browse/index.xhtml?](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

[filters=typeName%20in%20\(%22Address%22%2C%20%22EmailAddress%22%2](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

Type	Summary	Owner	Threat Rating	Obs	F/P	Tags	Added	Modified
File	6843AE9EAC03F69DF301D024BDFEFCB8 : BB5E262794...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	04-07-2017	05-17-2017
File	5D44E3A13D8C976D30178688E8535EC5 : B032EDCE950...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-17-2017	05-17-2017
File	8ADCC9E5E9137612418B6042F028640E : C626A2BB695...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-17-2017	05-17-2017
File	135D87DC18F703238CA6E360DD6E050 : 156B0696EFA...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-11-2017	05-11-2017
File	96CC23B77C36CECC34ADE9B740B7887 : 1B334DE892...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-11-2017	05-11-2017
File	32747103D34B6E773F81E24091D8E80D : EF12A5ED85C...	ThreatConnect Resear...	☹☹☹	-	-	Palestine Kaspersagent Palestinian Au...	05-04-2017	05-04-2017

Import Hash Results c66f88d2d76d79210d568d7ad7896b45

Type	Summary	Owner	Threat Rating	Obs	F/P	Tags	Added	Modified
File	A8FC19B2C8FE81B09813292D31EC1EB : 9B0E22652AA...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-17-2017	05-17-2017
File	980B1125805CCC351F3ABDE4FCE133E0 : 54822379B07...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-17-2017	05-17-2017
File	016EB60BDAD949C95BC2929F80D174B3 : C61A1F633D...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-17-2017	05-17-2017
File	FBF143B2D34C43BF50D713054F5B6035 : F83028A2D90...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-11-2017	05-11-2017
File	2DE2306A80B8A5B6C8E805E2FC5F3C5 : ECA953CAC4...	ThreatConnect Resear...	☹☹☹	-	-	Kaspersagent	05-03-2017	05-03-2017

Import Hash Results dcf3aa484253068d8833c7c5b019b07a

Analysis of those files uncovered two more imphashes,

0B4E44256788783634A2B1DADF4F9784

[[https://app.threatconnect.com/auth/browse/index.xhtml?](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

[filters=typeName%20in%20\(%22Address%22%2C%20%22EmailAddress%22%2](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

and [E44F0BD2ADFB9CBCABCAD314D27ACCF](#)

[\[https://app.threatconnect.com/auth/browse/index.xhtml?](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

[filters=typeName%20in%20\(%22Address%22%2C%20%22EmailAddress%22%2](https://app.threatconnect.com/auth/browse/index.xhtml?filters=typeName%20in%20(%22Address%22%2C%20%22EmailAddress%22%2)

, for a total of 20 malicious files. These additional samples behaved similarly to the initial files; testproj.exe dropped benign decoy files and started malicious executables. The malicious executables all called out to the same URLs on windowsnewupdates[.]com.

These malware samples leverage the user agent string “OPAERA,” the same one identified in the [Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA](#)

[\[http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/\]](http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/) blog. Although the

command and control domain was different from those in the report, the POST and GET requests were similar and included /dad5/ in the URL string. In addition, the malware samples included the kasper PDB string reported by Unit 42, prompting us to conclude that we were likely looking at new variants of KASPERAGENT.

The Decoy Files

Several of the decoy files appeared to be official documents associated with the Palestinian Authority - the body that governs the Palestinian Territories in the Middle East. We do not know whether the files are legitimate Palestinian Authority documents, but they are designed to look official. Additionally, most of the decoy files are publicly available on news websites or social media.

The first document - dated April 10, 2017 - is marked “Very Secret” and addressed to Yahya Al-Sinwar, who Hamas elected as its leader in Gaza in February 2017. Like the photo displayed in the first decoy file we found, this document references the death of Mazen Fuqaha. The Arabic-language text and English translation of the document are available in ThreatConnect [here](#)

[<https://app.threatconnect.com/auth/document/document.xhtml?document=4219292>]. A screenshot of the file is depicted below.



The second legible file, dated April 23, has the same letterhead and also is addressed to Yahya al-Sinwar. This file discusses the supposed announcement banning the rival Fatah [<https://en.wikipedia.org/wiki/Fatah>] political party, which controls the West Bank, from Gaza. It mentions closing the Fatah headquarters and houses that were identified as meeting places as well as the arrest of some members of the party.

التاريخ / 2017/04/23م

سري جدا جدا


الاخ/ يحيى السنوار.. "ابو ابراهيم" حفظة الله ورعاه
السلام عليكم ورحمة الله وبركاته ،،

الموضوع / بخصوص اعلان حركة فتح تنظيم محظور في قطاع غزة

بداية نهديكم اطيب التحيات ،ونسأل الله ان يصلكم كتابنا هذا وانتم في اتم الصحة والعافية ، اما بعد ..
* نعلمكم اننا على اتم الجهوزية لتطبيق القرار فور اعلانه .
* تم حصر المقرات التابعة لحركة "فتح" ومنازل بعض النشطاء التي تستخدم لادارة النشاطات
الحركية التي سيتم اغلاقها فور صدور القرار مباشرة .
* تم حصر القيادات والعناصر الفاعلة الذين سيتم اعتقالهم فور صدور القرار .

وتفضلوا بقبول فائق التقدير والاحترام ،،

العبد سامي عودة
مدير عام جهاز الأمن الداخلي



Looking at the Infrastructure

We don't know for sure who is responsible for this campaign, but digging into the passive DNS results led us to some breadcrumbs. Starting with [195.154.110\[.\]237](https://app.threatconnect.com/auth/indicators/details/address.xhtml?address=195.154.110.237&owner=Common+Community)

[<https://app.threatconnect.com/auth/indicators/details/address.xhtml?address=195.154.110.237&owner=Common+Community>], the IP address which is hosting the command and control domain

windowsnewupdates[.]com, we found that the host is on a dedicated server.

The screenshot shows the 'TCS - DomainTools v1.0' interface. At the top, it displays 'windowsnewupdates.com Thu, 08 Jun 2017 13:29:36 GMT'. Below this is a table with columns for 'IP', 'Nameserver', and 'Registrar'. A secondary table provides details for the domain:

Action	N
Action In Words	New
Action Date	2017-03-23
Domain	WINDOWSNEWUPDATES.COM
Post IP	195.154.110.237 ↗ +
Pre IP	

ThreatConnect DomainTools Integration Results

Using our Farsight DNSDB integration, we identified other domains currently and previously hosted on the same IP.

The screenshot shows the ThreatConnect interface for IP 195.154.110.237. It features a navigation bar with 'THREATCONNECT INTELLIGENCE' and a search bar. Below the IP address, there are tabs for 'Overview', 'Tasks', 'Activity', 'Reverse DNS', 'Associations', and 'Spaces'. The 'Reverse DNS' section shows a table of resolved domains:

Resolved	Resolution
04-23-2017 12:45 GMT	www.windowsnewupdates.com
04-23-2017 12:42 GMT	windowsnewupdates.com
04-19-2017 14:47 GMT	www.windowsnewupdates.com
04-19-2017 14:45 GMT	windowsnewupdates.com

The 'Passive DNS' section shows a table of historic domains:

Host	First Seen Resolution	Last Seen Resolution
windowsnewupdates.com	Wed Mar 22 16:37:42 UTC 2017	Mon May 22 11:15:53 UTC 2017
ns1.windowsnewupdates.com	Wed Mar 22 16:37:42 UTC 2017	Mon May 22 11:15:53 UTC 2017
ns2.windowsnewupdates.com	Wed Mar 22 16:37:42 UTC 2017	Mon May 22 11:15:53 UTC 2017
ns1.apfile2box.com	Thu Jun 23 18:02:54 UTC 2016	Mon May 22 05:26:14 UTC 2017
www.windowsnewupdates.com	Wed Mar 22 17:06:17 UTC 2017	Wed May 17 19:30:22 UTC 2017

Reverse DNS and Passive DNS results for 195.154.110[.]237

Two of the four domains that have been hosted at this IP since 2016 -- upfile2box[.]com and 7aga[.]net -- were registered by a freelance web developer in Gaza, Palestine. This IP has been used to host a small number of domains, some of which were registered by the same actor, suggesting the IP is dedicated for a single individual or group's use. While not conclusive, it is intriguing that the same IP was observed hosting a domain ostensibly registered in Gaza AND the command and control domain associated with a series of targeted attacks leveraging Palestinian Authority-themed decoy documents referencing Gaza.

Targeting Focus?

Just like we can't make a definitive determination as to who conducted this campaign, we do not know for sure who it was intended to target. What we do know is that several of the malicious files were submitted to a public malware analysis site from the Palestinian Territories. This tells us that it is possible either the threat actors or at least one of the targets is located in that area. Additionally, as previously mentioned, the decoy document subject matter would likely be of interest to a few different potential targets in the Palestinian Territories. Potential targets such as Hamas who controls the Gaza strip and counts Mazen Fuqaha and Yahya al-Sinwar as members, Israel which is accused of involvement in the assassination of Mazen Fuqaha [<https://www.nytimes.com/2017/03/27/world/middleeast/mazen-fuqaha-hamas-killing-israel.html>], and the Fatah party of which the Prime Minister and President of the Palestinian Authority are members.

The campaign corresponds with a period of heightened tension in Gaza. Hamas, who has historically maintained control over the strip, elected Yahya al-Sinwar - a hardliner from its military wing - as its leader in February. A Humanitarian Bulletin [<https://unispal.un.org/DPA/DPR/unispal.nsf/0/AC8C02B3FA96AA208525811CC>

published by the United Nations' Office for the Coordination of Humanitarian Affairs indicates in March 2017 (just before the first malware samples associated with this campaign were identified in early April) Hamas created "a parallel institution to run local ministries in Gaza," further straining the relationship between Hamas and the Palestinian Authority who governs the West Bank. After this announcement, the Palestinian Authority cut salaries for its employees in Gaza by 30 percent and informed Israel that it would no longer pay for electricity provided to Gaza

[<https://www.nytimes.com/2017/04/27/world/middleeast/palestinian-authority-hamas-gaza-electricity.html>] causing blackouts throughout the area and escalating tensions between the rival groups. Then, in early May (two days after the last malware sample was submitted) the Palestinian Authority held local elections [<http://abcnews.go.com/International/wireStory/palestinian-west-bank-local-elections-test-fatah-party-47389952>] in the West Bank which were reportedly seen as a test for the Fatah party. Elections were not held in Gaza.

All of that is to say, the decoy documents leveraged in this campaign would likely be relevant and of interest to a variety of targets in Israel and Palestine, consistent with previously identified KASPERAGENT targeting patterns. Additionally, the use of what appear to be carefully crafted documents at the very least designed to look like official government correspondence suggests the malware may have been intended for a government employee or contractor who would be interested in the documents' subject matter. More associated indicators, screenshots of many of the decoy documents, and descriptions of the activity are available via the March - May 2017 Kasperagent Malware Leveraging WindowsNewUpdates[.]com Campaign [<https://app.threatconnect.com/auth/campaign/campaign.xhtml?campaign=4219181>] in ThreatConnect.

Categories: [Blog](#) , [Featured Article](#) , [Threat Research](#)

ABOUT THE AUTHOR



The ThreatConnect Research Team: is an elite group of globally-acknowledged cybersecurity experts, dedicated to tracking down existing and emerging cyber threats. We scrutinize trends, technology and socio-political motivators to develop comprehensive knowledge of the cyber landscape. Then, we share what we've learned so that you can protect your organization, and your team can take precise action against threats.