KASPERAGENT Malware Campaign resurfaces in May Election

(1) threatconnect.com/blog/kasperagent-malware-campaign/

6/14/2017

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 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 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, stikerscloud[.]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.

The samples we identified leverage the same user agent string "OPAERA", 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

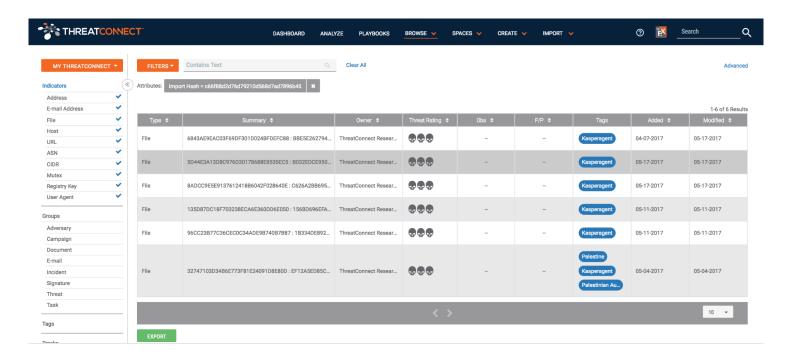
We didn't start out looking for KASPERAGENT, but a file hit on one of our YARA rules for an executable designed to display a fake XLS icon - one way adversaries attempt to trick targets into thinking a malicious file is innocuous. The

first malicious sample we identified (6843AE9EAC03F69DF301D024BFDEFC88) had the file name "testproj.exe" and was identified within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" and was identified within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" and was identified within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within an archive file (4FE7561F63A71CA73C26CB95B28EAEE8) with the name "testproj.exe" lizible within a constant with the name "testproj.exe" lizible within a constant with the name "testpr

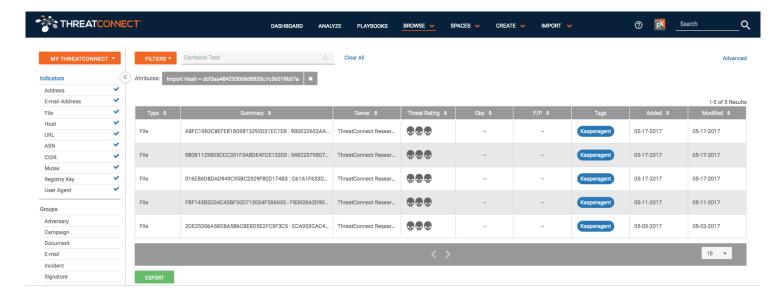
We detonated the file in VxStream's automated malware analysis capability and found testproj.exe dropped a benign Microsoft Word document that pulls a jpg file from treestower[.]com. Malwr.com observed this site in association with another sample that called out to mailsinfo[.]net - a host identified in the Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA blog. That was our first hint that we were looking at KASPERAGENT.

The jpg pulled from treestower[.]com 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 (vlc.exe) - runs when the photograph is displayed, using the YouTube icon and calling out to several URLs on windowsnewupdates[.]com. 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 and DCF3AA484253068D8833C7C5B019B07.



Import Hash Results c66f88d2d76d79210d568d7ad7896b45



Import Hash Results dcf3aa484253068d8833c7c5b019b07a

Analysis of those files uncovered two more imphashes, 0B4E44256788783634A2B1DADF4F9784 and E44F0BD2ADFB9CBCABCAD314D27ACCFC, 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 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. A screenshot of the file is depicted below.

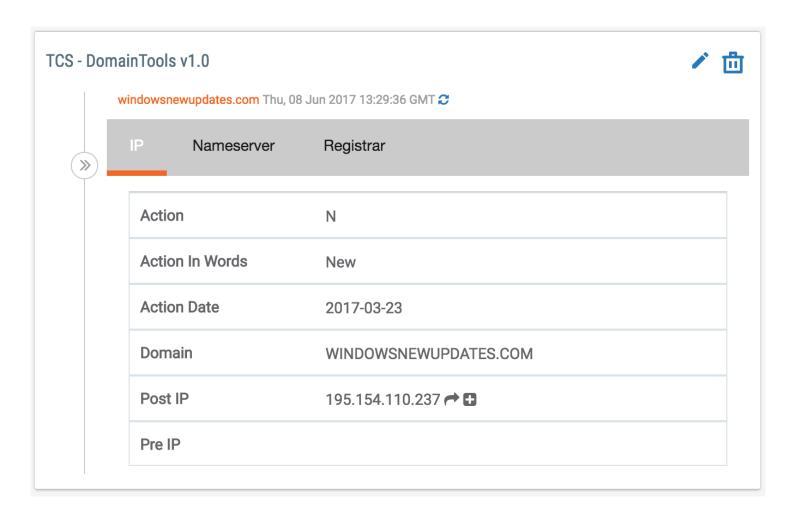


The second legible file, dated April 23, has the same letterhead and also is addressed to Yahya al-Sinwar. This file discusses the supposed announcement banning the rival Fatah political party, which controls the West Bank, from Gaza. It mentions closing the Fatah headquarters and houses that were identified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



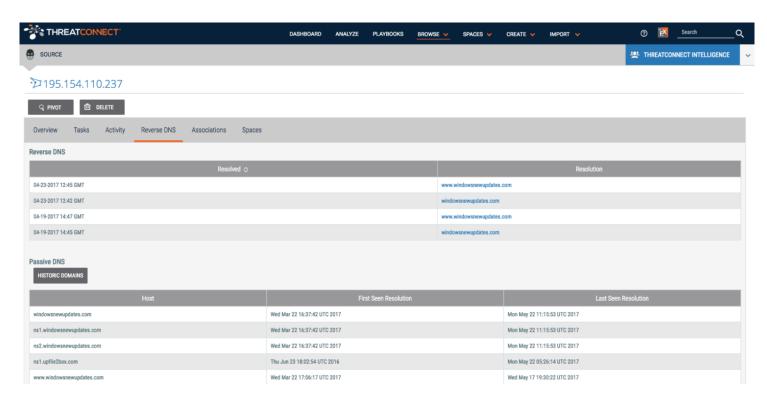
Looking at the Infrastructure

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, the IP address which is hosting the command and control domain windowsnewupdates[.]com, we found that the host is on a dedicated server.



ThreatConnect DomainTools Integration Results

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



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, 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 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 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 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 in ThreatConnect.