Targeted Attacks on Oil and Gas Supply Chain Industries in the Middle East

zscaler.com/blogs/security-research/targeted-attacks-oil-and-gas-supply-chain-industries-middle-east

Cybercriminals are known to look to current events to make their schemes and campaigns more engaging and relevant to unsuspecting victims. These events don't need to be global in nature, and are often only of local or regional interest. This helps the bad actors narrow their target hoping for a greater chance of success.

So when the Abu Dhabi National Oil Company (ADNOC) terminates engineering, procurement and construction (EPC) contracts it had previously awarded, attentive cybercriminals have new fodder for another scheme.

Since July 2020, the Zscaler ThreatLabZ team has observed an increase in targeted attacks against multiple supply chain-related organizations in the oil and gas sector in the Middle East. We discovered multiple instances of malicious PDF files sent as email attachments and were used to distribute an information-stealing Trojan, AZORult, to these organizations.

In this blog, we describe the details of this campaign, explaining the attack vectors, the malware distribution strategy, and the threat attribution.

Distribution strategy

The attack chain begins with an email that appears to be from an official working at the ADNOC and is targeted at officials working in the supply chain and government sectors in the Middle East.

Each email in this campaign has an attached PDF file. This PDF contains download links on the first page that lead to legitimate file sharing sites, such as wetransfer and mega.nz where a ZIP archive is hosted. The ZIP archive contains a malicious and packed .NET executable that will decrypt, load, and execute the embedded AZORult binary. Figure 1 shows a graphical representation of the attack flow.

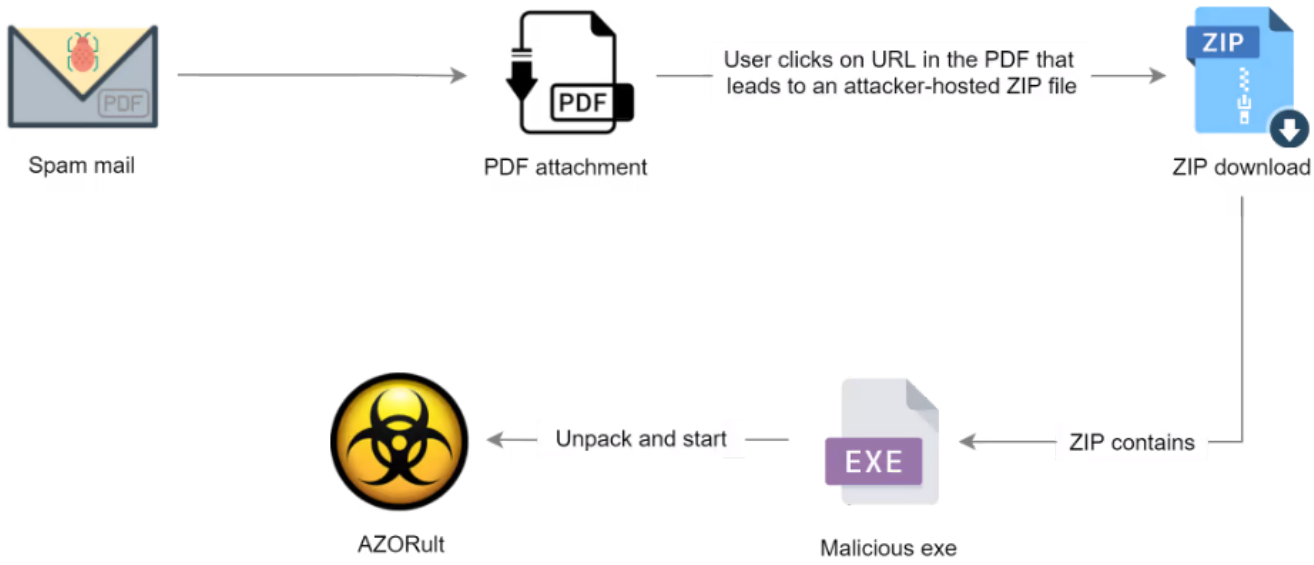


Figure 1: The flow of attack

Email analysis

Figure 2 shows an email message that pretends to come from a senior chemist of lab operations of ADNOC Sour Gas.

RFQ-VENDOR 3 YEARS SUPPLY CONTRACT (RENEWAL OF LTPA 62431092)

SS sales sigma <salessigma87@gmail.com>
To Sreekumar G
Cc mona.alameri.adnoc.ae@keemail.me; vijay.m.steadfastprojects.com@tuta.io
This message has extra line breaks.
RFQ-VENDOR 3 YEARS SUPPLY CONTRACT (RENEWAL OF LTPA 62431092).pdf
770 KB

Dear Sir,

We invite you to submit your Most Competitive Offer to execute and complete the whole works as described herein,

under the terms of the Sub-Contract Conditions and in accordance with the Main Conditions of Contract.

Bill of Quantities, Specifications and Drawings for the above mentioned Tender Project can be found in the attachment link.

Kind Regards

Figure 2: A fake email sent to officials in the supply chain industry in the Middle East.

In all the cases, the emails were sent from Gmail-based address. The two Gmail addresses observed in the attacks were:

The threat actor also leveraged anonymous email services from Tutanota to create emails registered with keemail.me and tuta.io which were also used in this email campaign.

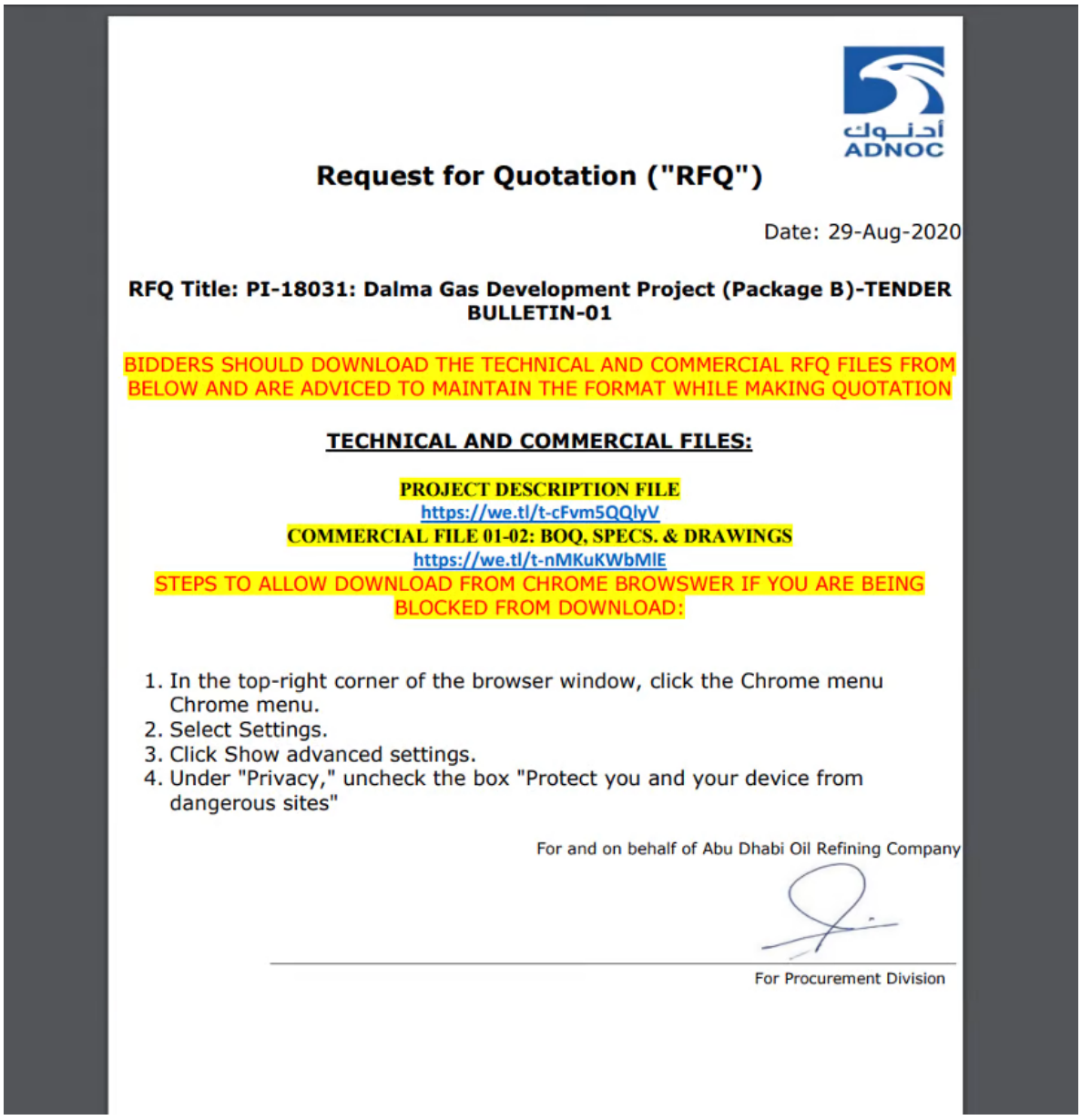
The PDF files attached to the email are multipage documents (containing 14 pages) that appear to be Requests for Quotations (RFQ) for supply contracts and legal tenders for various projects related to ADNOC and the Doha airport. The decoy documents are carefully crafted to appear legitimate for social engineering purposes. The first page of each document contains the instructions to access the specifications and drawings using embedded download links that lead to malicious ZIP archives as described in the attack flow above.

Some examples of the content in the PDFs include:

PDF Filename: PI-18031 Dalma Gas Development Project (Package B) -TENDER BULLETIN-01.pdf

MD5 hash: e368837a6cc3f6ec5dfae9a71203f2e2

Figure 3 shows a PDF that pretends to be a legitimate Request for Quotation (RFQ) related to the Dalma gas development project. It bears the logo of ADNOC at the top right and the first page contains the malicious download links.



Request for Quotation ("RFQ")

Date: 29-Aug-2020

RFQ Title: PI-18031: Dalma Gas Development Project (Package B)-TENDER BULLETIN-01

BIDDERS SHOULD DOWNLOAD THE TECHNICAL AND COMMERCIAL RFQ FILES FROM BELOW AND ARE ADVICED TO MAINTAIN THE FORMAT WHILE MAKING QUOTATION

TECHNICAL AND COMMERCIAL FILES:

PROJECT DESCRIPTION FILE
https://we.tl/t-cFvm5QQlyV
COMMERCIAL FILE 01-02: BOQ, SPECS. & DRAWINGS
https://we.tl/t-nMKuKWbMlE
STEPS TO ALLOW DOWNLOAD FROM CHROME BROWSWER IF YOU ARE BEING BLOCKED FROM DOWNLOAD:

1. In the top-right corner of the browser window, click the Chrome menu Chrome menu.
2. Select Settings.
3. Click Show advanced settings.
4. Under "Privacy," uncheck the box "Protect you and your device from dangerous sites"

For and on behalf of Abu Dhabi Oil Refining Company

For Procurement Division

Figure 3: The fake letter contained in the PDF associated with this attack.

PDF Filename: AJC-QA HAMAD INTERNATIONAL AIRPORT EXPANSION, DOHA.pdf

MD5 hash: abab000b3162ed6001ed8a11024dd21c

Figure 4 shows a PDF that pretends to be a Request for Quotation for Hamad International Airport expansion plan for Doha and supposedly comes from a supply chain trading contractor in Qatar.

Figure 4: The fake RFQ for a local airport expansion project.

Threat attribution

The threat actor is specifically interested in Middle East targets, such as organisations in the supply chain and government sectors of the Middle East, especially the United Arab Emirates (UAE) and Qatar.

Based on the target recipients of the email, the contents of the email, and the attached PDF files, along with the metadata and infrastructure analysis, we conclude that this is a targeted attack on organisations in the Middle East.

Metadata analysis

After investigating the metadata of PDF files, we were able to discover several PDFs that we associate with the same threat actor. The distribution method has been used in the wild from January 2020 through May 2020 in low volume.

Starting from July 2020, we observed an increase in the activity of this threat actor, returning with a new campaign.

The metadata of the PDF files indicates that they were generated using Microsoft Office Word 2013. The only unique author names used in all the PDF samples were:

Donor1

Mr. Adeel

Figure 5 shows an example of the metadata for the PDF file with the MD5 hash e368837a6cc3f6ec5dfae9a71203f2e2.

ExifTool file metadata

MIMEType	application/pdf
ModifyDate	2020:08:29 21:28:47-07:00
Language	en-US
Producer	Microsoft® Word 2013
Author	Donor1
CreateDate	2020:08:29 21:28:47-07:00
PageCount	14
Linearized	No
Creator	Microsoft® Word 2013
FileTypeExtension	pdf
PDFVersion	1.5
FileType	PDF

Figure 5: The metadata of one of the PDFs used in this campaign.

The complete list of all the PDF samples identified in this campaign is provided in the Appendix.

Infrastructure analysis

In addition to the contents of the emails and the documents that were used for threat attribution, we can also infer from the Command and Control (C&C) infrastructure that the threat actor has specifically chosen a C&C server that blends with the theme.

The C&C server in the samples we discovered was crevisoft.net.

At the time of analysis, this domain was resolving to the IP address 167.114.57.136. We observed that this domain, when accessed directly, would redirect to a service consulting company from Egypt hosted at crevisoft.com as shown in Figure 6.

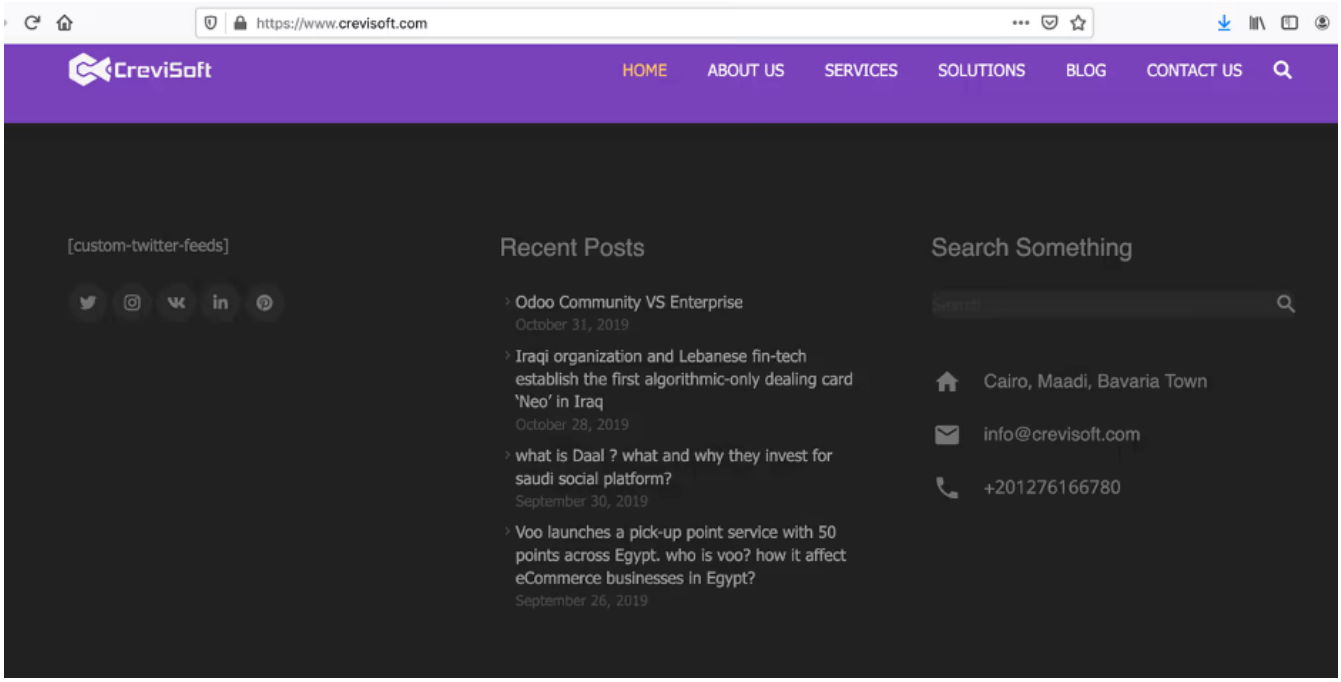


Figure 6: A legitimate Middle East-based site hosted at crevisoft.com.

All of the following four domains would redirect to the above domain:

crevisoft.net

cis.sh

crevisoft.org

crevisoft.co

With a high confidence level, we can conclude that this threat actor is interested in stealing information and gaining access to infrastructure of supply chain-related organisations located in the Middle East.

Technical analysis of the .NET payload

For the purpose of technical analysis, we will consider the .NET binary with MD5 hash: 84e7b5a60cd771173b75a775e0399bc7

This payload, which is present inside the downloaded ZIP archive, is a packed and obfuscated .NET binary.

Based on static analysis, we can see that the payload pretends to be a Skype application with spoofed metadata as shown in Figure 7.

```
14  [assembly: AssemblyVersion("8.61.4.0")]
15  [assembly: Guid("bf98d332-2178-4f14-a3a3-b555cc771c77")]
16  [assembly: ComVisible(false)]
17  [assembly: AssemblyTrademark("")]
18  [assembly: CompilationRelaxations(8)]
19  [assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
20  [assembly: AssemblyFileVersion("8.61.4.0")]
21  [assembly: AssemblyCopyright("(c) 2020 Skype and/or Microsoft")]
22  [assembly: AssemblyTitle("Skype")]
23  [assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAttribute.DebuggingModes.DisableOptimizations |
      DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints | DebuggableAttribute.DebuggingModes.EnableEditAndContinue)]
24  [assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
25  [assembly: AssemblyProduct("Skype")]
26  [assembly: AssemblyCompany("Skype Technologies S.A.")]
27  [assembly: AssemblyDescription("Skype")]
28
```

Figure 7: Metadata of the main .NET executable.

Upon execution, it unpacks another payload that is embedded in the resource section. Figure 8 shows the custom algorithm that decrypts the payload using a hardcoded key “GXR20”.

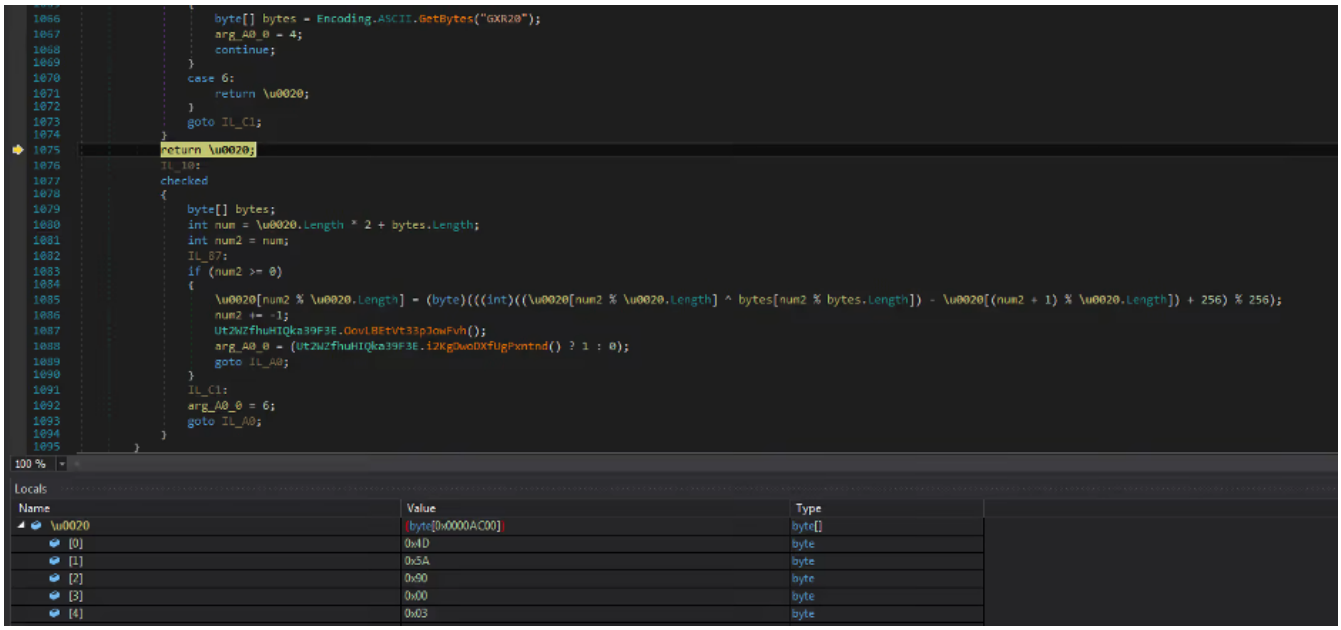


Figure 8: The subroutine used to decrypt the second stage .NET DLL.

Second stage

Figure 9 shows the decrypted payload, which is a .NET DLL with the **MD5 hash** 0988195ab961071b4aa2d7a8c8e6372d and the name Aphrodite.dll

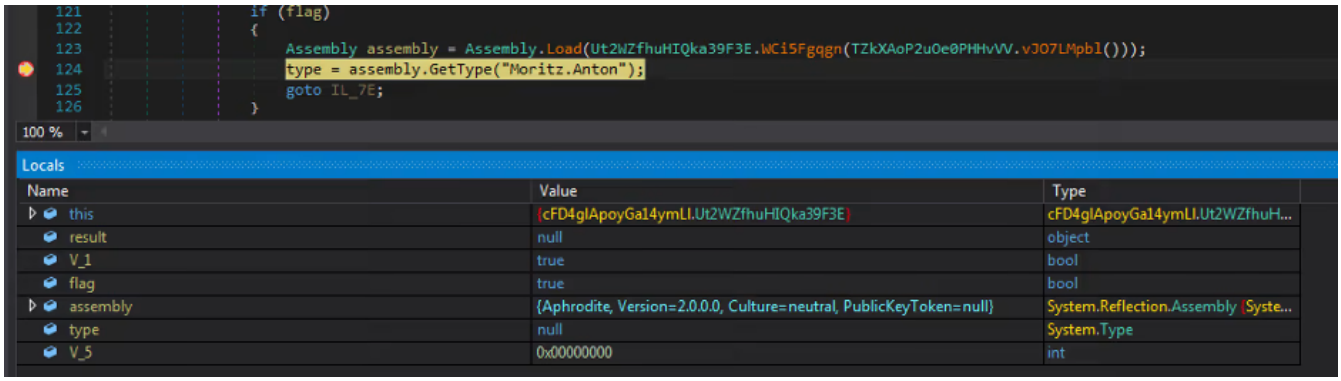


Figure 9: The unpacked and loaded second stage DLL called Aphrodite.

The code execution is transferred to the DLL by creating an object for class named “Mortiz.Anton” along with the following three parameters, as shown in Figure 10.

ugz1: “ddLPjs” (name of the bitmap image resource)

ugz3: ”KKBxPQsGk” (the decryption key)

projName: “Skype” (name of the project of main executable)

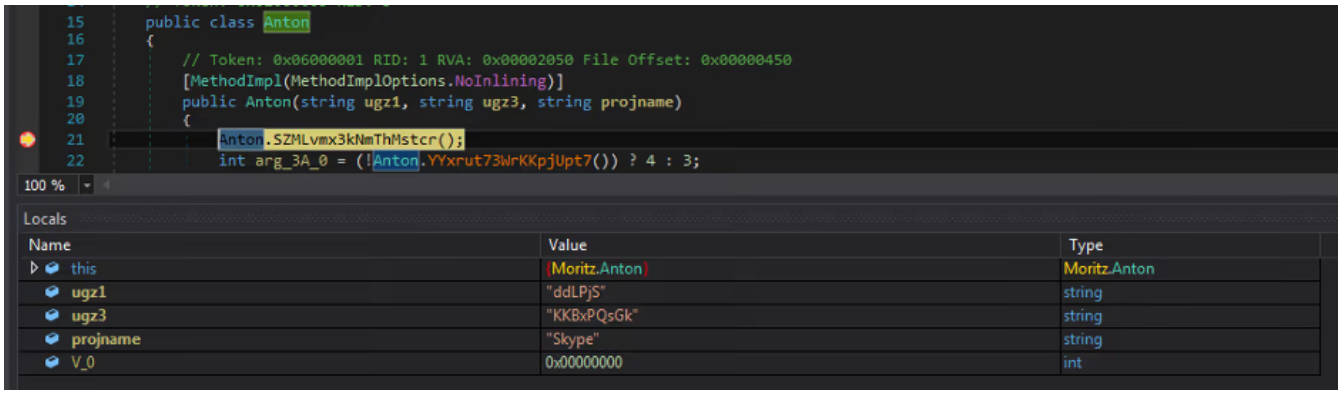


Figure 10: The code control passed to the Aphrodite DLL.

This DLL further unpacks another binary, which is embedded as a bitmap image in the resource section of the main executable, as shown in Figure 11.

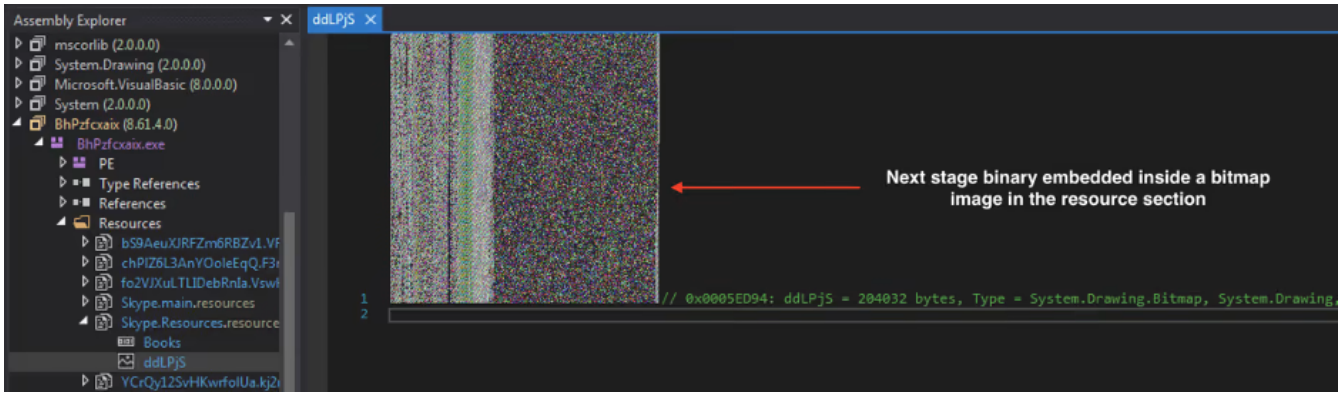


Figure 11: The bitmap image inside the resource section that contains the next stage payload.

Similar to the second stage (Aphrodite), it is also encrypted with a custom algorithm. The custom algorithm is based on XOR using the key indicated by the parameter ugz3**.**

Third stage

The resulting unpacked binary is a .NET DLL with **MD5 hash** ae5f14478d5e06c1b2dc2685cbe992c1 and the name Jupiter.

The code control is transferred to the third stage DLL via a call to one of its routines as shown in Figure 12.

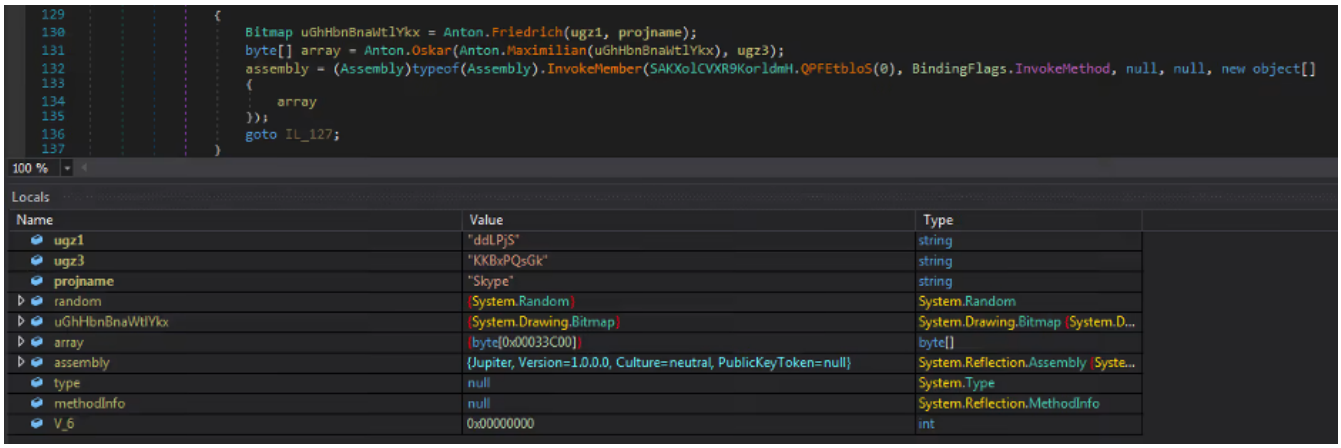


Figure 12: The unpacked and loaded third stage DLL called Jupiter.

This third stage DLL uses various methods to detect the presence of a virtualization or an analysis environment.

Evasion techniques

Below is a summary of the methods used by this DLL to detect the analysis environment.

Registry checks:

Registry key: "HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 0\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0"

Value: "Identifier"

Data contains: "VBOX" OR "VMWARE" OR "QEMU"

Registry key: "HARDWARE\\Description\\System"

Value: "SystemBiosVersion"

Data contains: "VBOX" OR "QEMU"

Registry key: "HARDWARE\\Description\\System"

Value: "VideoBiosVersion"

Data contains: "VIRTUALBOX"

Checks if key present: "SOFTWARE\\Oracle\\VirtualBox Guest Additions" OR "SOFTWARE\\VMware, Inc.\\VMware Tools"

Registry key: "HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 1\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0"

Value: "Identifier"

Data contains: "VMWARE"

Registry key: "HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 2\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0"

Value: "Identifier"

Data contains: "VMWARE"

Registry key: "SYSTEM\\ControlSet001\\Services\\Disk\\Enum"

Value: "0"

Data contains: "VMWARE"

Registry key: "SYSTEM\\ControlSet001\\Control\\Class\\{4D36E968-E325-11CE-BFC1-08002BE10318}\\0000"

Value: "DriverDesc"

Data contains: "VMWARE"

Registry key:

"SYSTEM\\ControlSet001\\Control\\Class\\{4D36E968-E325-11CE-BFC1-08002BE10318}\\0000\\Settings"

Value: "Device Description"

Data contains: "VMWARE"

Registry key: "SOFTWARE\\VMware, Inc.\\VMware Tools"

Value: "InstallPath"

Data contains: "C:\\PROGRAM FILES\\VMWARE\\VMWARE TOOLS\\"

Wine environment detection:

Checks if the export functions of kernel32.dll contains: wine_get_unix_file_name

Windows Management Instrumentation (WMI) query-based checks:

WMI Query: "SELECT * FROM Win32_VideoController"

Property: "Description"

Checks for the presence of the following keywords in the description field:

- "VM Additions S3 Trio32/64"
- "S3 Trio32/64"
- "VirtualBox Graphics Adapter"
- "VMware SVGA II"
- "VMWARE"

DLL name-based checks:

Checks for the presence of a DLL with the name: "SbieDll.dll" in the process address space.

Username-based checks:

Checks if the system username contains either of the following strings:

- "USER"
- "SANDBOX"
- "VIRUS"
- "MALWARE"
- "SCHMIDTI"
- "CURRENTUSER"

Filename or filepath-based checks:

FilePath contains: "//VIRUS" OR "SANDBOX" OR "SAMPLE" OR "C:\\file.exe"

Window class check:

"Afx:400000:0"

After all the above environment checks are performed, the AZORult payload (**MD5 hash:** 38360115294c49538ab15b5ec3037a77) is injected using the process hollowing technique in a new instance of the main process.

We will not describe the details of the functionality of AZORult information stealer since it is already well-documented in the public domain.

It is important to note that based on the flow of the code execution and the anti-analysis techniques used, the .NET packed payload appears to be created using the CyaX packer. More details about this packer can be found here.

Network communication

The final unpacked payload, AZORult, will perform information stealing activities on the machine and exfiltrate the information by sending an HTTP POST request to the URL: hxxp://crevisoft.net/images/backgrounds/ob/index.php

Upon inspection, we discovered that opendir was enabled on the C&C server as shown in Figure 13.

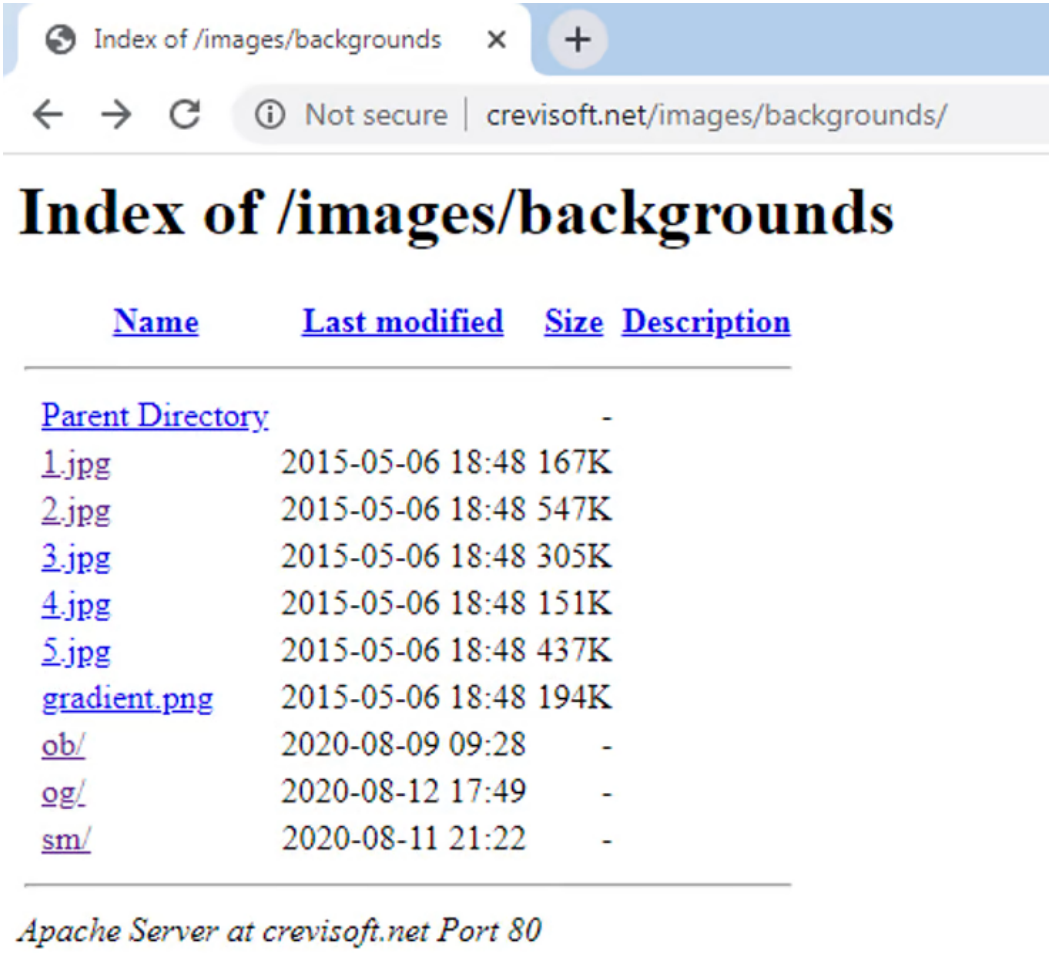


Figure 13: Opendir enabled on the C&C server.

The AZORult panel on the C&C server can be accessed at the URL: hxxp://crevisoft.net/images/backgrounds/ob/panel/admin.php.

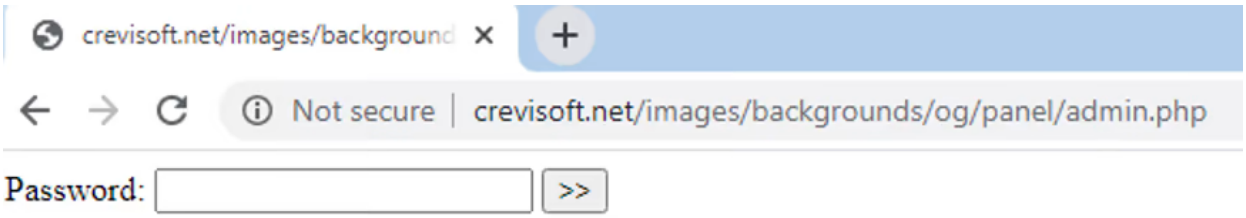


Figure 14: The AZORult panel

PHP mailer script

Among other artifacts we discovered on the C&C server, we found a PHP mailing script deployed at hxxp://crevisoft[.]net/images/-/leaf.php.

This enables the threat actor to send emails using the C&C server's SMTP.

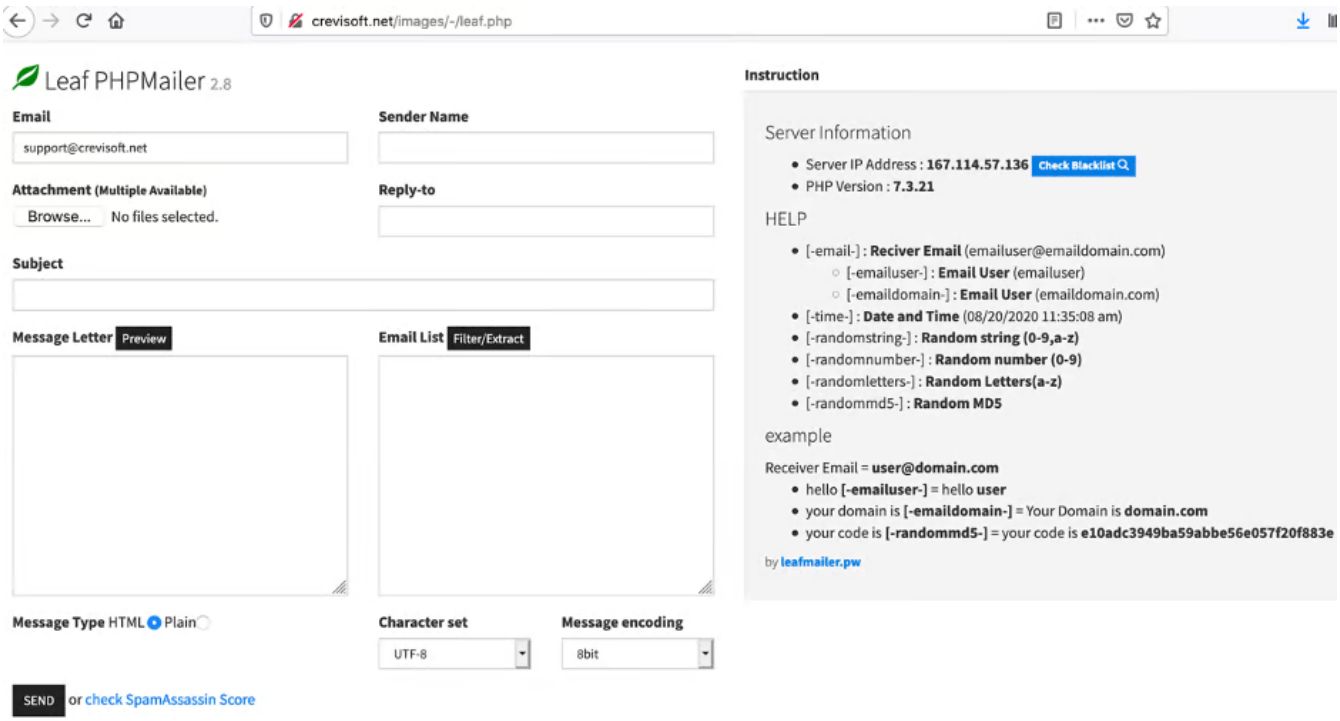


Figure 15: The PHP mailing script on the C&C server.

Zscaler Cloud Sandbox detection

Figure 16 shows the Zscaler Cloud Sandbox successfully detecting this .NET-based threat.

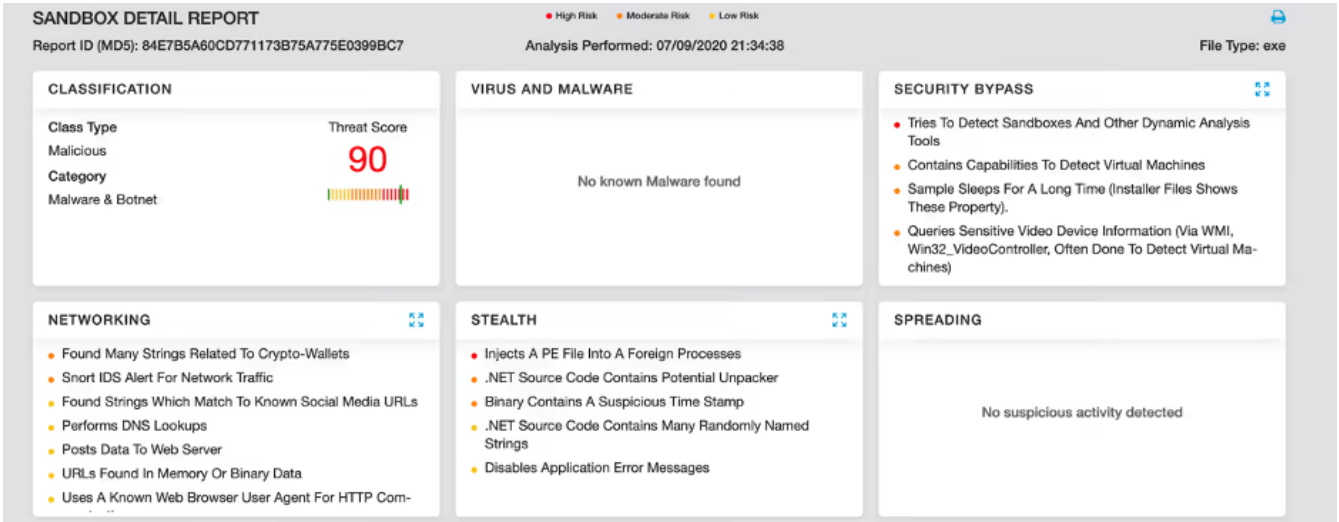


Figure 16: Zscaler Cloud Sandbox detection.

In addition to sandbox detections, Zscaler's multilayered cloud security platform detects indicators at various levels, as seen here:

Win32.PWS.Azorult

Win64.PWS.Azorult

PDF.Downloader.Azorult

Conclusion

This threat actor is targeting employees in the supply chain industries in Oil and Gas sector in the middle east region. As always, users should be cautious when receiving emails out of the blue, even if those emails appear to be related to something you are interested in, such as a legal tender for a project which might appear relevant. And always be wary of links embedded inside file formats such as PDF since these links could lead to download of malicious files on your system.

The Zscaler ThreatLabZ team will continue to monitor this campaign, as well as others, to help keep our customers safe.

MITRE ATT&CK TTP Mapping

ID	Tactic	Technique
T1566.001	Spearphishing Attachment	Uses PDF attachments containing malicious URLs
T1204.002	User Execution: Malicious File	User opens pdf file. Click the URL link. Downloads ZIP file. Extracts zip file and executes the binary.
T1140	Deobfuscate/Decode Files or Information	Strings and other data are obfuscated in the payload.
T1036.005	Masquerading: Match Legitimate Name or Location	File names used related to projects directly linked to the Middle East.
T1027.002	Obfuscated Files or Information: Software Packing	Payloads are packed with a multilayer packer.
T1497	Virtualization/Sandbox Evasion	Uses Registry, WMI, UserName-based anti-VM techniques
T1134.002	Access Token Manipulation: Create Process with Token	One of AZORult capabilities
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	One of AZORult capabilities
T1140	Deobfuscate/Decode Files or Information	One of AZORult capabilities
T1573.001	Encrypted Channel: Symmetric Cryptography	One of AZORult capabilities
T1083	File and Directory Discovery	One of AZORult capabilities
T1070.004	Indicator Removal on Host: File Deletion	One of AZORult capabilities
T1105	Ingress Tool Transfer	One of AZORult capabilities
T1057	Process Discovery	One of AZORult capabilities
T1055.012	Process Injection: Process Hollowing	One of AZORult capabilities
T1012	Query Registry	One of AZORult capabilities
T1113	Screen Capture	One of AZORult capabilities
T1082	System Information Discovery	One of AZORult capabilities

T1016	System Network Configuration Discovery	One of AZORult capabilities
T1033	System Owner/User Discovery	One of AZORult capabilities
T1124	System Time Discovery	One of AZORult capabilities
T1552.001	Unsecured Credentials: Credentials In Files	One of AZORult capabilities

Indicators of compromise

Scheduled task names

Naming convention: “Updates\<random_string>”

Updates\YJSlNpkH

Updates\WWOsRUUn

Updates\NcojkRtJmDPru

XML file names

Scheduled tasks are created using dropped XML files in %temp% directory with random names.

C:\Users\user\AppData\Local\Temp\tmp9AA2.tmp

C:\Users\user\AppData\Local\Temp\tmp23B7.tmp

C:\Users\user\AppData\Local\Temp\tmp24CC.tmp

Dropped filenames

Files are dropped in the “AppData\Roaming” directory with the same name as a scheduled task.

C:\Users\User\AppData\Roaming\YJSlNpkH.Exe

C:\Users\User\AppData\Roaming\WWOsRUUn.Exe

C:\Users\user\AppData\Roaming\NcojkRtJmDPru.exe

File hashes

PDF hashes

Author: Donor1

e368837a6cc3f6ec5dfae9a71203f2e2

741f66311653f41f226cbc4591325ca4

fe928252d87b18cb0d0820eca3bf047a

8fe5f4c646fd1caa71cb772ed11ce2e5

d8e3637efba977b09faf30ca49d75005

c4380b4cd776bbe06528e70d5554ff63

34cae3ae03a2ef9bc4056ca72adb73fc

363030120a612974b1eb53cc438bafcb

2710cc01302c480cd7cd28251743faf0

1693f1186a3f1f683893b41b91990773

7a016c37fa50989e082b7f1ca2826f04

709895dd53d55eec5a556cf1544fc5b9

5d9ed128316cfa8ee62b91c75c28acd1

c2ac9c87780e20e609ba8c99d736bec1

269cfd5b77ddf5cb8c852c78c47c7c4c

653f85816361c108adc54a2a1fadadcf

6944f771f95a94e8c1839578523f5415

8e5c562186c39d7ec4b38976f9752297

3d019ede3100c29abea7a7d3f05c642b

67f178fd202aee0a0b70d153b867cb5e

39598369bfca26da8fc4d71be4165ab4

70a92fdba79eaca554ad6740230e7b9a

9db3d79403f09b3d216ee84e4ee28ed3

bafdeef536c4a4f4acef6bdea0986c0b

8d7785c8142c86eb2668a3e8f36c5520

653e737fd4433a7cfe16df3768f1c07e

ebdcb07d3de1c8d426f1e73ef4eb10f4

d258ba34b48bd0013bfce3308576d644

a74c619fd61381a51734235c0539e827

6f1bd3cb6e104ed6607e148086b1e171

cf04d33371a72d37e6b0e1606c7cd9a2

ede5fa9b9af1aeb13a2f54da992e0c37

5321cd5b520d0d7c9100c7d66e8274e1

de521f9e4bc6e934bb911f4db4a92d36

36e5726399319691b6d38150eb778ea7

1c5cb47fd95373ade75d61c1ae366f8b

b7b41d93709777780712f52a9acf7a26

62a05b00c7e7605f7b856c05c89ee748

b520f4f9d87940a55363161491e69306

40c1156d98c39ac08fd925d86775586d

Author: Mr. Adeel

f2319ddb303c2a5b31b05d8d77e08b4e

24e67f40ccb69edb88cc990099ef2ffe

54fc7650a8b5c1c8dc85e84732a6d2c7

9cf615982d69d25b1d0057617bd72a95

e9dfa14e4f6048b6f3d0201b2f3c62fe

abab000b3162ed6001ed8a11024dd21c

5c857bf3cf52609ad072d6d74a4ed443

73ddf9f8fc3dc81671ea6c7600e68947

3510cbf8b097e42745cfb6782783af2b

694a6568b7572125305bdb4b24cebe98

7fa5028f2394dcea02d4fdf186b3761f

2260d015eacdc14e26be93fbc33c92aa

d51d5e4c193617fa676154d1fe1d4802

912dbb9e0400987c122f73e0b11876c0

0f4cd9e8111d4eeda89dbe2ce08f6573

d03fb3e473bd95c314987a1b166a92ed

549a06cb43563dad994b86e8f105323a

80149a26ee10786d6f7deaf9fb840314

c7ced41f38b2d481d1910663a14fbec4

3ce6cc6dee4563eb752e55103cdb84d4

ZIP hashes

6d0241bc7d4a850f3067bc40124b3f52

cdfde809746759074bcd8ba54eb19ccd

40b5976eb7ddd1d372e34908f74ba0c4

93c8ed2915d8a3ff7285e0aa3106073e

2b719eeca275228fbead4c1d3016b8e4

Exe hashes

42aec0b84a21fa36fc26b8210c197483

02ae44011006e358a3b1ccbd85ba01f2

131772a1bb511f2010da66c9c7dca32f

7860c138e3b8f40bfb6efec08f4a4068

3bcbe4d2951987363257a0612a107101

328aa4addb7e475c3721e2ae93391446

84e7b5a60cd771173b75a775e0399bc7

3c83b0fe45e15a2fd65ed64a8e1f65e9

f626e64f57d3b8c840a72bbfbe9fb6ca

fcf7a9b93cffddf0a242a8fc83845ee3

Unpacked file hashes

0988195ab961071b4aa2d7a8c8e6372d - Aphrodite

Ae5f14478d5e06c1b2dc2685cbe992c1 - Jupiter

38360115294c49538ab15b5ec3037a77 - Azorult

Unique PDF file names

Author: Donor1

RFQ #88556524.pdf

ADNOC RFQ 97571784 - Purchase - core store Mussafah - Tehnical and Commercial.pdf

ALJABER-GROUP-RFQ-38982254237312018-848000071984-03-19-Rev-1.1.pdf

Dalma Gas Development Project (Package B) -TENDER BULLETIN-01.pdf

RFQ-VENDOR 3 YEARS SUPPLY CONTRACT (RENEWAL OF LTPA 62431092).pdf

Author: Mr. Adeel

RFQ-ALJ-HAMAD INTERNATIONAL AIRPORT EXPANSION, DOHA.pdf

RFQ-HAMAD INTERNATIONAL AIRPORT EXPANSION, DOHA QATAR.pdf

RFQ-HAMAD INTERNATIONAL AIRPORT EXPANSION, DOHA.pdf

RFQ#ENQ34640-ALJ24.pdf

AJC-QA HAMAD INTERNATIONAL AIRPORT EXPANSION, DOHA.pdf

C&C servers

hxxp://crevisoft[.]net/images/backgrounds/ob/index.php

hxxp://nsseinc[.]com/lingo/index.php

Email address

ZIP hosted URLs:

Author of PDF: Donor1

hxxps://we[.]tl/t-lBcWz3Rcbs

hxxps://mega[.]nz/#!Ov41xapb!M-COPorpfcQ7j1G61afFVruLbDVwzNfujRlwERqlIQw

hxxps://we[.]tl/t-P2Lt34YUcf

hxxps://we[.]tl/t-7XwI9xNjQj

hxxps://we[.]tl/t-AgAdhMTWIm

hxxps://mega[.]nz/file/fkImWKab#zvyeMmsYgGiu-hK-FT0o4OBozg0r4gWPRUtAr6iRvwM

hxxps://we[.]tl/t-utJr50o6uf

hxxp://bit[.]ly/32qQFah

hxxps://mega[.]nz/file/zsIB2aLK#pyTNpp8H4pZhpq0i7w0OB8itu3Rj_02n9BksARDrlzc

hxxps://mega[.]nz/#!nrozSBoL!Pc5ApemPW46RC8b0kgiTIyuIa0MnQV9GDUPXGK8__LM

hxxps://we[.]tl/t-TbbBN9VnEZ

hxxps://mega[.]nz/#!KuRElKZT!5F_FfxkyPI7tvJ-mnL7LppAU5X5wA1XbpTM-z8DpVB8

hxxps://mega[.]nz/file/q55WVlKB#zm3CTH6XEv63mwacATKpo2AMe7yjFmp-KpQXUBkhZJ4

hxxp://bit[.]ly/3a3CwSX

hxxps://we[.]tl/t-MFcMWYK7HL

hxxps://mega[.]nz/#!Tmw0EK5Q!zSLa_EII7Ti5sz-ca-plgqc4vZM7S813Hb9Yk5Jk81Y

hxxps://we[.]tl/t-0NIciPHf5y

hxxps://mega[.]nz/#!y6w1BAqS!DMfA221sRvIyqVqPNhsKMZEAtBNkjY_jLUWEmCpxMfo

hxxps://mega[.]nz/#!j2JSwQYb!LaAP2L2WBKLU3DlR6BViQxZ4b8fsmt53Hl3RKHMfb4w

hxxps://mega[.]nz/file/Ptp1CL6R#EvbG9Gh435cDmmXXyU1_l4dM3Bq9fP2B8VdjirGiK_c

hxxps://we[.]tl/t-feLBFQVV1P

hxxps://we[.]tl/t-ad5X6peqHj

hxxps://www[.]dropbox[.]com/s/cym2723azwnb364/ADNOC%202020%20REQUEST%20FOR%20QUOTATION-REQUEST%20FOR%20TENDER%20CODE%2076384_pdf[.]zip?dl=0

hxxps://we[.]tl/t-uwwupT1WNc

hxxps://mega[.]nz/#!K6xgGCYJ!1cJY91lIlLLrGGrDVVrkbb7vNRKL9CAFD4tB9_jP8ts

hxxps://mega[.]nz/#!yrBGmQBA!EhgekpU4VUafMvfJKlNVFej1KsgxYWv1mfzCKXejjEc

hxxps://we[.]tl/t-ZcyzrvcBkP

hxxps://mega[.]nz/file/GpB3VIyS#3-tKCJ8d-y782IN0570wHMMKQ244ttzBRpUmFXh6LZQ

hxxps://mega[.]nz/#!OvJFjQaY!UBgEDtTE_Gn4B4vYrn-d7rYeO5CBMTxt83NyXQGWh0E

hxxps://mega[.]nz/file/G5YmjCYJ#jvqrZX2ZLXn3SAI9nzf8w6mWtxTM4_fwx7VzHdqzfqM

hxxps://mega[.]nz/#!zygWnKAS!5kp8IWNec2HK-YPK2gk-hmLa416PZLtr6VpbNZediSk

hxxps://mega[.]nz/#!uu40wQxJ!HXlLJw7KDJgqnpwCzgrnBt9vu_W1-FZlSIvn0JU5rDw

hxxps://mega[.]nz/#!66hWzACL!_6klTwfD-JaSkwjWrKRIBqX1ghXr-SZGk1Utc2-VJPc

hxxps://www[.]aljaber-llc[.]com/projects/files/ALJABER-RFQ-38982254237312018-848000071984-04-23-Rev-1[.]1[.]zip

hxxps://we[.]tl/t-cJa4jY9Egz

hxxps://we[.]tl/t-Out44emJ9t

hxxps://we[.]tl/t-QuCLQY3cTh

hxxps://we[.]tl/t-nMKuKWbMlE

hxxps://mega[.]nz/file/f1RTVa4A#2uGmQV64RKkNYZEECYXFKjGPS-naIF2ZshufSgqsA_k

hxxps://we[.]tl/t-oAkwGNORsR

hxxps://we[.]tl/t-cFvm5QQlyV

hxxps://www[.]dropbox[.]com/s/5b0bti9r6xhf3pq/ADNOC%202020%20REQUIREMENT%20TENDER%20RFQ%2056774387_PDF[.]zip?dl=0

hxxps://we[.]tl/t-Didobux8kG

hxxps://we[.]tl/t-FkBOHwy1ME

hxxps://mega[.]nz/file/u7xRlS7T#l8L3NL_zi-JizZagSF-E1Gcj5I8ednV6YdqyWs5RnNo

hxxps://we[.]tl/t-XsVO5hewBu

Author of PDF: Mr. Adeel

hxxps://we[.]tl/t-NwSigkLd2E

hxxps://we[.]tl/t-wQB6ioE8dL

hxxps://we[.]tl/t-u3NL7Wnplr

hxxps://we[.]tl/t-zC6Wz4CpfZ

hxxps://we[.]tl/t-5wQSJsFUlC

hxxps://we[.]tl/t-egfvdBvESW

hxxps://we[.]tl/t-2a9aq4LJSn

hxxps://we[.]tl/t-4BnTk2Hwiv

hxxps://we[.]tl/t-hSqtTJDi1f

hxxps://we[.]tl/t-1VyVEAtzAf

hxxps://we[.]tl/t-E1iDs5Bghr

hxxps://we[.]tl/t-YlbV0AIU5b

hxxps://we[.]tl/t-1yLti4IfaN

hxxps://we[.]tl/t-dGN9sRTnch

hxxps://we[.]tl/t-spOqYklJIQ

hxxps://we[.]tl/t-cunxjPBouY

hxxps://we[.]tl/t-39SvbwCY2E

hxxps://we[.]tl/t-9RVc3dflK6

hxxps://we[.]tl/t-aBUVx3EMdx

hxxps://we[.]tl/t-XdOjUbrcK8

hxxps://we[.]tl/t-MkUZugwABd

hxxps://we[.]tl/t-ikxwkPtSBi

hxxps://we[.]tl/t-1hWeuMe1h7

hxxps://we[.]tl/t-2L7ajlJSCG

hxxps://we[.]tl/t-HZygDd5TUJ

hxxps://we[.]tl/t-MtgNnMbTij