

Global Phishing Campaign Targets Energy Sector and its Suppliers

 intezer.com/blog/research/global-phishing-campaign-targets-energy-sector-and-its-suppliers/

July 7, 2021

Written by [Nicole Fishbein](#) and [Ryan Robinson](#) - 7 July 2021



Get Free Account

[Join Now](#)

Top Blogs

Top Cyber Threats to the Telecom Industry

In our interconnected society, the telecom industry is responsible for keeping the world connected 24/7.... [Read more](#)

Top Cyber Threats to the Manufacturing Sector

Manufacturers are building automated workflows for alert triage, incident response, and threat hunting to meet... [Read more](#)

Automate Alert Triage and Response Tasks with Intezer EDR Connect

Integrate with SentinelOne, CrowdStrike, and More One of the biggest pain points of cyber security... [Read more](#)

Our research team has found a sophisticated campaign, active for at least one year, targeting large international companies in the energy, oil & gas, and electronics industries. The attack also targets oil & gas suppliers, possibly indicating that this is only the first stage in a wider campaign. In the event of a successful breach, the attacker could use the compromised email account of the receipt to send spear phishing emails to companies that work with the supplier. Thus using the established reputation of the supplier to go after more targeted entities.

The attackers use typosquatted and spoofed emails to launch the attack. The campaign spreads via phishing emails tailored to employees at each company being targeted. The contents and sender of the emails are made to look like they are being sent from another company in the relevant industry offering a business partnership or opportunity. Each email has an attachment, usually an IMG, ISO or CAB file. These file formats are commonly used by attackers to evade detection from email-based Antivirus scanners. Once the victim opens the attachment and clicks on one of the contained files an information stealer is executed.

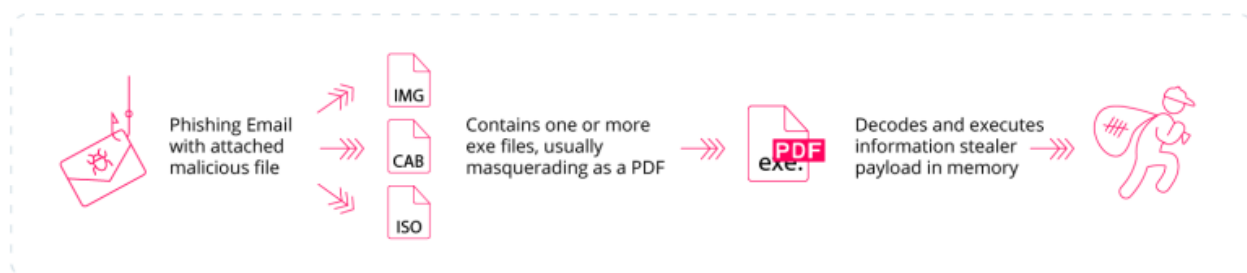
Below we describe the attack vector, the attackers' motives and tactics used in this campaign, and how you can protect your systems from this attack.

Key Findings

- The campaign uses spoofed or typosquatted emails to make them look like part of a normal business-to-business (B2B) correspondence.
- The attached file is primarily an IMG, ISO or CAB file containing information stealer malware.
- The dropped malware is generally able to steal private information, log keyboard strokes and steal browsing data.

Phishing Campaign Delivers Stealers in ISO, IMG or CAB Files

INTEZER



Attack Flow

The Campaign

Recently, we have identified a number of IMG files with names related to the oil & gas and energy industries. Inside these image files are predominantly .NET malware. Upon further investigation the distribution method for this malware appears to be spear phishing emails, with either an IMG, ISO, or CAB file included as an attachment and sent to specific targets. The IMG/ISO files are part of the Universal Disk Format (UDF) which are disk images commonly used for DVDs. Cabinet (CAB) files are a type of archive file. In most of these emails the file name and icon of the attachment mimics a PDF. The purpose is to make the file look less suspicious, enticing the targeted individual to open and read it.

The campaign targets companies from around the world, including the United States, United Arab Emirates (UAE) and Germany, but its primary targets are South Korean companies. The targeted industries are wide-ranging but mostly focused on the energy sector.

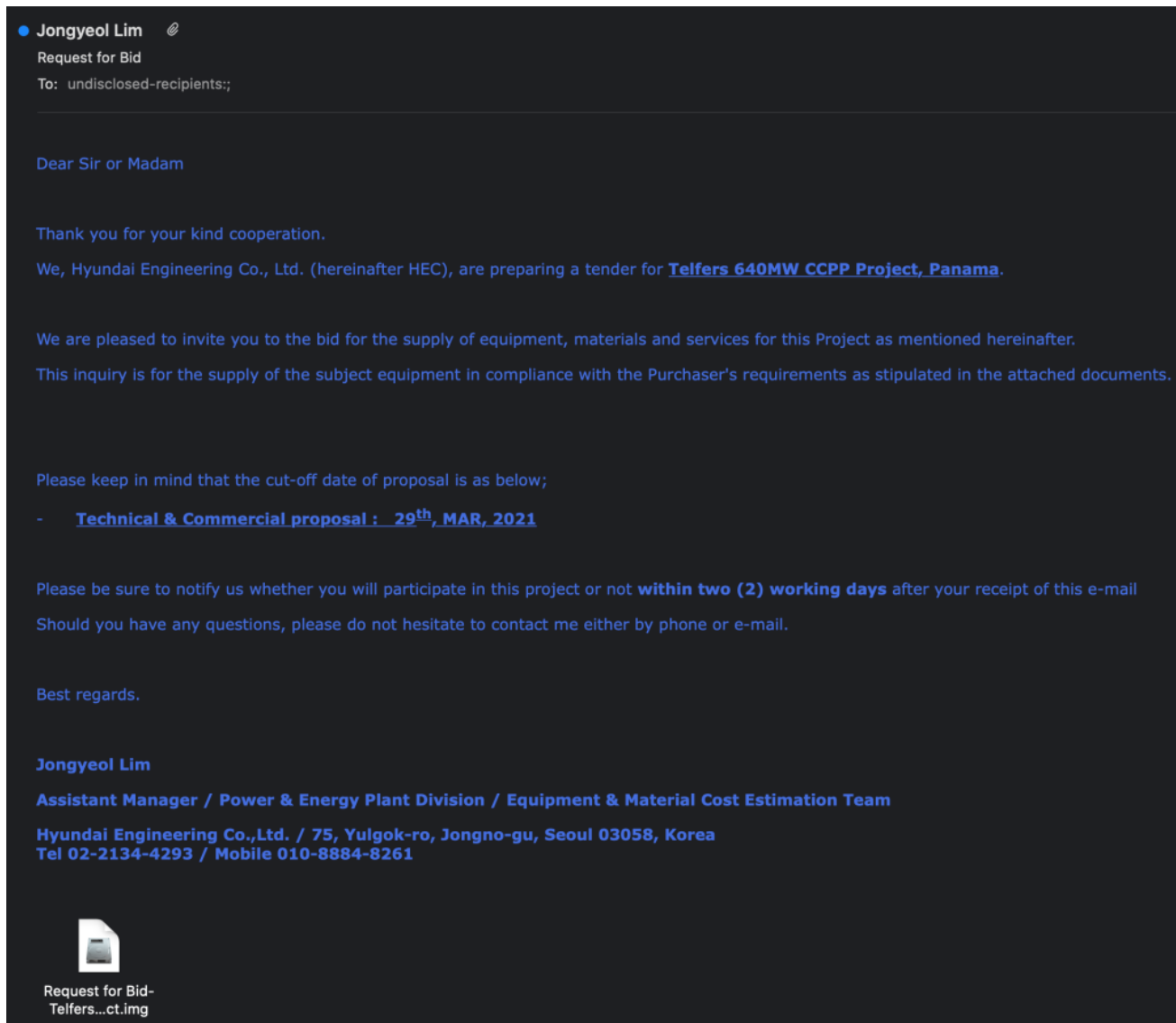
- Energy
- Oil & Gas
- Information Technology
- Manufacturing
- Media

The Emails

The emails are formatted to look like valid correspondence between two companies. This extra effort made by the attacker is likely to increase the credibility of the emails and lure victims into opening the malicious attachments. The emails use social engineering tactics such as making references to executives, using physical addresses, logos and emails of legitimate companies. They also include requests for quotations (RFQ), contracts, and referrals/tenders to real projects related to the business of the targeted company.

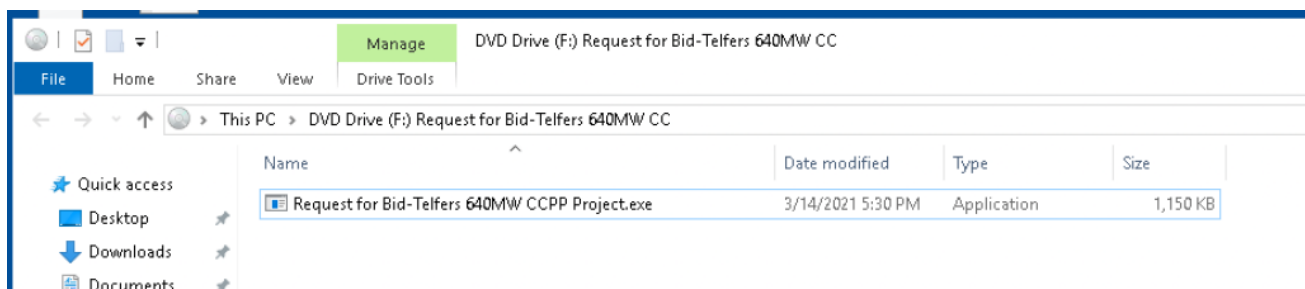
The content of the emails demonstrates that the threat actor is well-versed in business-to-business (B2B) correspondence. The recipient email addresses of these emails range from generic email handles such as “**info@target_company[.]com**” or “**sales@target_company[.]com**” to specific people within companies. This suggests that for some companies they have likely managed to gather more intelligence during reconnaissance than others.

An example of one of the emails involved in the campaign (image below) uses a combined cycle power plant (CCPP) project in Panama as a lure. The email pretends to be sent from Hyundai Engineering Co (HEC). The email asks the receiver to submit a bid for the supply of equipment in the project and states that more details and requirements can be found in the attached file (containing the malware). The email presents a strict deadline for which the request for the bid should be submitted.



Phishing email inviting recipient to participate in a project.

Upon opening the disk image file the target is presented with an executable.



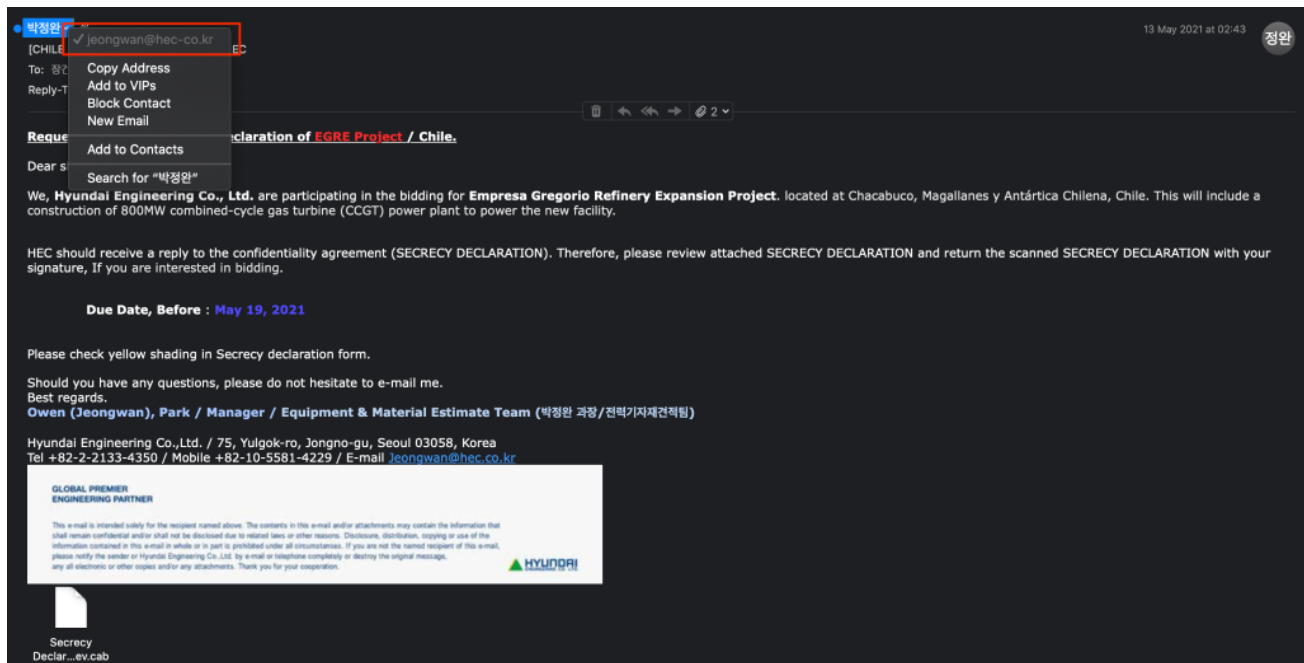
Malicious file contained in the disk image.

Email Tactics

Typosquatting

In several emails it appears the sender domains have been typosquatted in order to increase the credibility of the spear phishing attempt. Typosquatted domains are a technique used to social engineer email recipients into thinking an email has been sent from a trusted entity. This technique is performed by registering a domain name which mimics a legitimate domain. When viewed quickly it can increase the chances of the recipient thinking that the email has been sent from a legitimate company.

In this campaign, many of the typosquatted domains mimic South Korean companies with legitimate domains in the format of <company.co.kr>. Typosquatting is achieved by registering a domain without the second level “.co” and instead registering the domain as <company-co.kr>. One example of this is the domain <hec-co.kr>, registered by the attackers to typosquat the legitimate domain for the company Hyundai Engineering (hec.co.kr). The typosquatted email from “Hyundai Engineering” invites the recipient to reply to a confidentiality agreement with respect to a refinery expansion project.



Email sent from typosquatted domain (jeongwan@hec-co.kr).

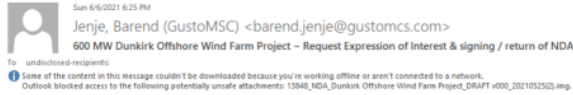
Another typosquatted email that caught our attention was supposedly sent by Barend Jenje from GustoMSC, asking to return a signed non-disclosure agreement (NDA). The attachment was just an IMG file containing a malware executable.

GustoMSC is based in The Netherlands, specializing in offshore equipment and technology for the oil & gas industry. On June 14, 2021, GustoMSC posted an alert on their site warning users that the company’s domain was being typosquatted and scammers were sending emails on behalf of their employees.

The email below references the **Dunkirk offshore wind farm project** to add credibility to the message. The project was granted to the Éoliennes en Mer de Dunkerque (EMD) consortium by the French government in June 2019. The consortium is made up of several

companies, two of which are mentioned in the email: EDF Renouvelables and Enbridge. In recent news, the companies announced their decision to move forward with the development of the project beginning in the second half of 2021.

It would make sense then why the attackers name dropped this project, due to its recent developments and also because the offshore wind farm is under the occupation of GustoMSC.



Gentlemen:

Greetings of the day!

GustoMSC is bidding for Dunkirk offshore wind farm Project located in Grand Port Maritime of Dunkirk, France being developed by EDF Renewables and Enbridge Éolien France S.à r.l.. For this bidding, we are in requirement of quotation for equipment and / Services. As per the project guidelines, we need to sign a **NDA (Non-Disclosure Agreement)** before sending the formal RFQ documents for quotation. We request you to kindly sign the attached **NDA** to enable us to proceed further to share the formal enquiry to you.

Attached is the NDA (Non-Disclosure Agreement) for use in the, 600 MW Dunkirk offshore wind farm project. Kindly review and provide your compliance on priority by **EOD June, 14th, 2021**.

After reviewing, please fill in as below:

1st Page - All fields highlighted in yellow
Date
Company's legal name
Entity type
Registered company address

Last Page - Bottom right fields
Insert Counter party Name (company's Legal Name)
By: place signature of authorized company representative
Name: Full and complete name of signatory

Once all fields are filled, please remove the yellow highlight. Return completed and signed NDA to this as soon as possible. Should you have any questions, please contact the undersigned.

Also, please advise the name and contact details to whom we shall be sending the Inquiry. Following details are required :-

- Physical Address
- Phone Number
- Email Address
-


With kind regards

GustoMSC B.V.

Phishing email impersonating GustoMSC.

Email Spoofing

Many email addresses in this campaign are spoofed by the actor. Email spoofing is another tactic that is used to social engineer targets into opening emails. Email spoofing is done by sending an email with forged headers to suggest that the email is sent from a trusted or legitimate entity. An example of a spoofed email from this campaign pretends to come from a company called Haesung Tech, seen below.

● (주) 해성테크 

9 April 2021 at 03:49

성

RFQ [긴급] 견적 요청의 건 _ 해성테크

To: undisclosed-recipients;;

안녕하십니까 해성테크 입니다.

긴급 견적요청 드립니다.

되도록이면 금일 중으로 견적서 회신 부탁드립니다.

(주) 해성테크
주소 : 경남 창원시 마산회원구 봉암북13길 31
haesungtech@haesungtech.com
Tel : 055-299-7642
Fax : 055-292-762



RFQ 견적요청_해
성190918.IMG

Spooled email pretending to be sent from Haesung Tech.

This email is clearly spoofed since inside the header the Sender Policy Framework (SPF) check does not pass. The reason for this is there is no DNS TXT record for **haesungtech.com** that defines a permitted sender. The SPF verdict is shown below.

```
Received-SPF: none (211.104.2.85: domain at haesungtech.com does not designate permitted sender hosts)
Authentication-Results: smf.febc.net;
  spf=none (211.104.2.85: domain at haesungtech.com does not designate permitted sender hosts) smtp.mailfrom=haesungtech@haesungtech.com
Received: from unknown (HELO server.ecomotorhk.com) (162.144.56.225)
```

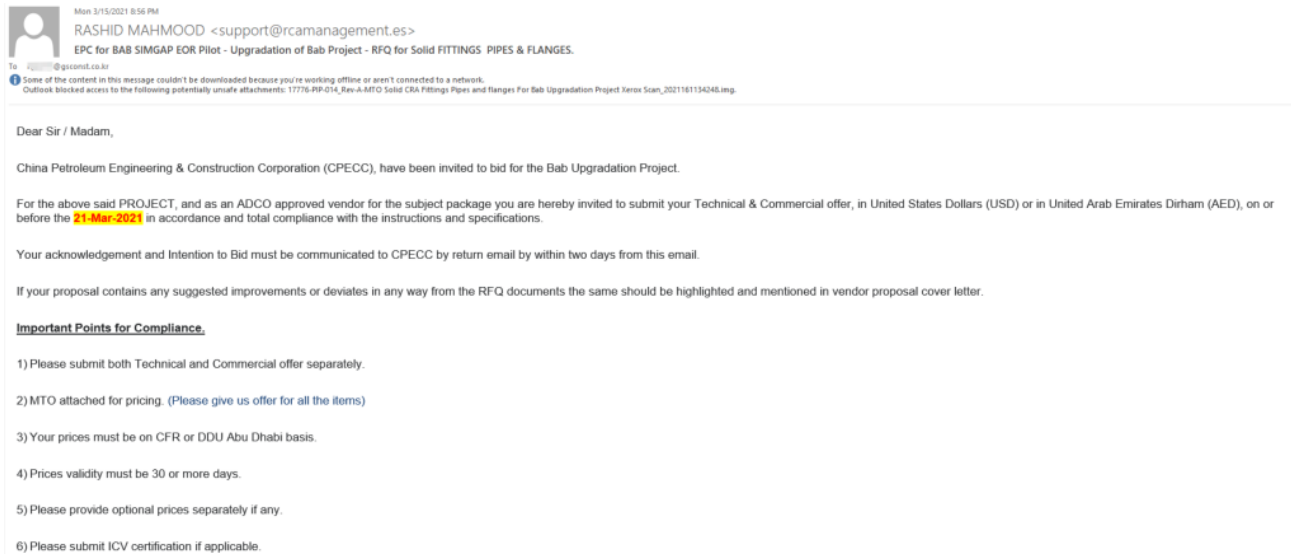
Sender Policy Framework (SPF) verdict.

The Malware

This campaign uses several known Remote Access Tools (RATs) and information stealing malware contained in the files attached to the phishing emails. Although the threats belong to different malware families, they do share a number of capabilities including: stealing private and banking information, logging keyboard strokes and stealing browsing data.

There are several known malware-as-a-service (MaaS) threats like Formbook and Agent Tesla used in this campaign. Other threats we have identified are Loki, Snake Keylogger and AZORult.

Each email has an attached file containing one or more executables encapsulated inside an IMG, ISO, or CAB file, each belonging to one of the threats mentioned above. In Windows 8 and Windows 10, simply double-clicking on virtual disk files will automatically mount its content. This feature is appealing for threat actors because it takes a small number of user clicks to execute the malware. In addition, traditional email defenders do not handle disk image files as well as more common formats such as ZIP files. Therefore, it's more likely that the malicious emails will end up in the inbox of the recipients without being blocked. One of the emails we analyzed was allegedly sent by Rashid Mahmood from China Petroleum Engineering & Construction Corporation (CPECC), a subsidiary of the China National Petroleum Corporation. The recipient of the phishing email works for a company called GS E&C, a Korean EPC contractor engaged in various global power plant projects.



Phishing email sent to GS E&C.

The email contains a reference to the expansion project of an oil field in Abu Dhabi called BAB. BAB is the oldest operating field in the United Arab Emirates (UAE). The receiver of this email, who works at GS E&C, is invited to submit both technical and commercial offers for the items described in the attached material take off (MTO) document (below).

7) Please provide ADNOC approval document.

PLEASE DOWNLOAD SPECIFICATIONS FROM THE ATTACHED FILE


Best Regard,

RASHID MAHMOOD

Project Buyer

BAB Integrated Facilities Project

中国石油工程建设有限公司海湾地区公司

 CHINA PETROLEUM ENGINEERING & CONSTRUCTION CORPORATION

Email: rashid.mahmood@cpecc.ae Website: www.cpecc.ae

Office Tel: Direct 971 (0)2-201-3412 Ext. 412 Fax. 971 (0)2-678-7799

Mobile 971 (0) 56-9900694

Second part of the phishing email sent to employee at GS E&C.

There is a typo in the email below. Instead of “regional headquarters” the address says “Reginal Headquarter.” In addition to this mistake, the address provided is the actual address of CPECC in UAE.

Address: CPECC **Reginal Headquarter**

5th Floor, WAFRA Square Building, Al Reem Island Najmat,

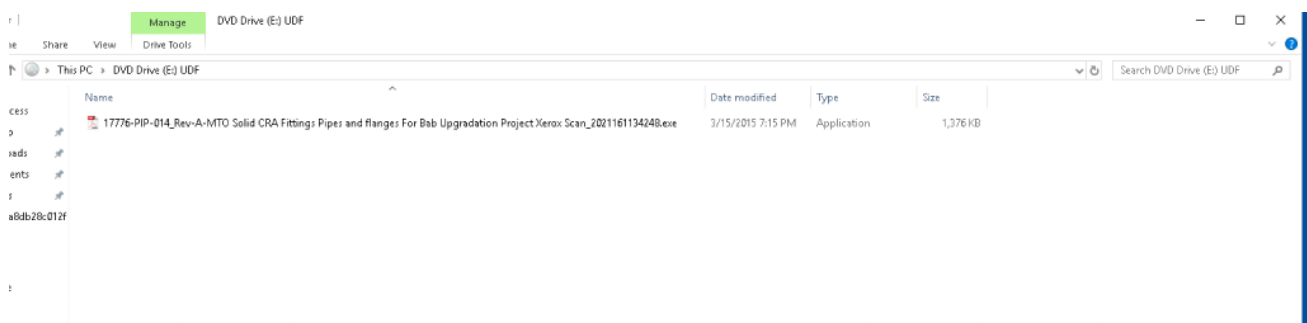
Al Reem Mall Intersection, P.O Box 127345, Abu Dhabi UAE

 Please consider the environment, before printing this email

The information contained in this email and any attachments may be legally privileged and confidential.

Phishing email with a typo.

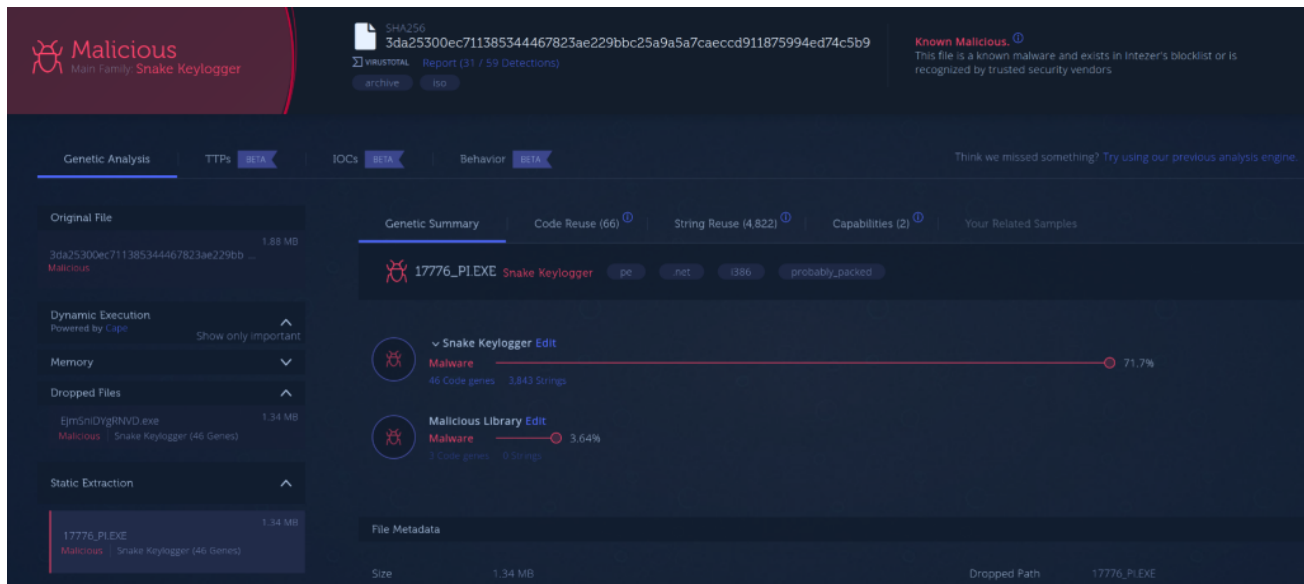
Though the attached file has a seemingly complementary name related to the contents of the email, it is actually an IMG file that contains Snake Keylogger malware. Once the user double-clicks on the IMG file, the content of the file is mounted, as shown below, and the user can click the file to be executed.



Mounted disk image file with malicious Snake Keylogger binary masquerading as PDF.

To bypass detection from standard Antiviruses, the execution of the malware is fileless, meaning that it is loaded into memory without creating a file on disk. In this case, it performs the same loading and execution process used to load Agent Tesla as reported by BlackBerry.

We uploaded the attached file to [Intezer Analyze](#). The file contains a malicious PE file that shares code with other Snake Keylogger samples.



Genetic analysis of the ISO sample containing Snake Keylogger.

Targeting Companies in Religion Media Business

Among the targeted companies there is one that differs drastically from the others. The company is [FEBC](#), a religious Korean Christian radio broadcaster that reaches other countries outside of South Korea, many of these countries which downplay or ban religion. One of FEBC's goals is to subvert the religion ban in North Korea.

Recommendations

Treat emails with awareness and caution, especially emails that are received from outside your company's domain. Most importantly, don't open suspicious files or links.

Fileless malware is now very common. A recent [blog](#) by Panda Security states that fileless malware rates in 2020 increased by 888% over 2019. Therefore, it is important to ensure that your organization's security strategy includes software that is able to detect malware injected and executed in-memory. In case you come across a suspicious file, you can upload it to [Intezer Analyze](#) to get an immediate verdict (trusted or malicious) and malware family classification if it is indeed a malicious file. The platform supports a wide range of file formats, including Windows and Linux executables, scripts and documents.

To summarize, don't click on suspicious emails and make sure you have a solution that handles [fileless malware](#) in-memory effectively. Intezer Analyze can help you with the latter.

Intezer Analyze now supports non-executable files such as Microsoft Office documents, PDF files, and scripts such as PowerShell and VBS.

IoCs

Email: 1c85618ef82808c9bcc6deddf93b66d6ee7a81b82c03341ecbf61d3ee4975bb3

Attached file: 74109522b38c609b4c576eecd644ffe544fcdc9a6494a9683f8eea6fb9e0bc7

Email: cd77a054500efdac4d39d743ad83f963c738d6f2b6b53f5c4b5818d34742f02b

Attached file:

3da25300ec711385344467823ae229bbc25a9a5a7caeccd911875994ed74c5b9

Email: 8877b6a829967924063e85120bf22b2ccc511fa25e376b479213020a15482bf6

Attached file: 0dc594a10793d93e26584d8dcd4d811c4b2ccb017b86eb1119380f17e3606f85

Email: b51e83fd2583c8e92ef34f6b8d23e07aaa82eedcf2db4b68e667f3a52c8862f5

Attached file: 079c7d83465481952407f3da954e08a5f165ff5480e2a51c32505088e78750f5

Attached file: 53e3ae371a3e329c6ed4942eb6cc51007c53008e3b9da6fccaecbed8f68f2ffa

Attached file: 96ff156bd7b09ec5a6216f43c0de578aafa9a8103832a401ce156e2ee918f580

Email: ff5be1c9c0ee11ceca68c10a9bcd1f8a995be8e3f89ed17a4933adde010ac3ad

Attached file:

d5080a9391b2ad1a75deeee81db15be47be2b0742378f633081eb4c9f81226ad

Email: a722bde3892eeafdd285b6e9aabc67f0ad8dc8abe4035a8ff11671a7c2a68b1

Attached file: 01970569f16e4adfdd4afb50d7a85327e8eb6abd7cb61a446e4a6f1010835968

Attached file: 0ab00782d02cb0e817b0237007b6b7f81139ff6ded17bc42fbf277e929b77ccf

Email: 3d8d4fbf52301ea8dca5602d6c86da3d82fd659074d7868938064e84c7ad424a

Attached file: ee7a4274d02042c8e516de2695ced13f4623c96377762f088d7795d5b0b2bd6f

Email: 0ea3575eed95cf60b1efb487a350a9fa24fd77482e881020a9a0f77220a6ad33

Attached file:

102adafddb589d6739ce8a489054825a9a958baa01e87b95eebdc302675a3bd9

Email: 9644169dee32d60f41d8d4e1f3dfb45a930ad3efd993fe941647549cf5e924dd

Attached file:

e2adb897c29a67295a2b411c47ee76e1e9ce1e27dccf259bc42a84c481ae41ce

Email: a03c0a2b6458cf55ee800291cf6b4698d1450bddd6d9e3e02f963c465004ac5c

Attached file: f1e85b9f7b1c2a6ce9da528dbfe2c66f0a0f513f39411dbf7bb7d4d917e1ba99

Email: 0840cff0a98daa3962236913952b7b16896cae63af24fa99e46f3371c0e1ca49

Attached file: 6a99c482b1634f3d0c775f4c8a0d1bb04cd24a0f54f1f48d1ee2697f5bf1c6c3

Email: 86ebf42301074e2907578e98dc20c46f6ecf9789503c625e2b2abfcb2af847b2

Attached file: 079c7d83465481952407f3da954e08a5f165ff5480e2a51c32505088e78750f5

Attached file: 53e3ae371a3e329c6ed4942eb6cc51007c53008e3b9da6fccaecbed8f68f2ffa

Attached file: 96ff156bd7b09ec5a6216f43c0de578aafa9a8103832a401ce156e2ee918f580

Email: 5384a56a7d814aea903c33bfd602a3e3d5bc637b6e3bc0bd4568d4b7b99db2ad

Attached file: f873b017cb3063a499db2874275e4797b8412ccd1300d29f4f1af03d66ee6700

Email: 8620f85ffd045187ffbc5d7e70df01d8a04e7fc5c69048b152f2b7284d20caf1

Attached file: 06a3fe74ff3dd352db742ac96c6fbd0da1a0d98164dda2a6637e809ec0f48b35

Email: b552939890305a0a0d2c9af8973a7d04b1593d9f512c0cc485a0b987f4293d97

Attached file: 8e2c23037b36f558920f626e7ef8767daa55734551238eb8816abd144f27db45

Attached file: 9c55cc8f7acc09b5de745ec99b0c60862f7975eab77420e41b5c9d1351114cd9

Attached file: d90f2a4a97cf6523e868f67356df7fc08581912c37e8f1f6ee16f2220eabdbb6

Email: 5db134f3aa187e74903a732b1bd55419977d66c63a55ae8952d908b8b0bc2616

Attached file:

713da8a5f0b2ee6a477a57b90834d4ae4637723ad817ffc5a53e5c86792e8ba4

Attached file: 7b57b59d06c7ef6cc6fa09fafdf427f2db5969d1b49041d1b7a992e47a9a2726

Attached file: b06cfcc8fabebb1bc83a4dfc91c0f9ba4e23c539018bb94fef1431745c0a2506

Email: 87b197032a6976c18f7f3df1df6e09cf9fd6a8e4cce3f35f51b2cf521b9ca278

Attached file: 7aacd968f2cfb23a8369712c0dc60bcabc7b7d7c0ebf69863f7643e6b90e656f

Attached file: 9e9ea32799bf9a246d76b11131abf71bbcffd3b79e026e440b221f6b1bdffe90

Email: 75ce82077ab9b2e18df87dae0e52270ae49fe20ec22f66fa3698b6fb75452e95

Attached file: 14ae4b4b66588af22cf569a90c94e9dd6e2af708ad9dc0efde0cd7d2a809fb51

Attached file: 60dc089158d86e9fb10ace29eb6afd7f23d001181e8a4a6ba5083c3597733a71



Nicole Fishbein

Nicole is a malware analyst and reverse engineer. Prior to Intezer she was an embedded researcher in the Israel Defense Forces (IDF) Intelligence Corps.



Ryan Robinson

Ryan is a security researcher analyzing malware and scripts. Formerly, he was a researcher on Anomali's Threat Research Team.