EMSISOFT | Blog

SECURITY ALERTS

Beware: New wave of malware spreads via ISO file email attachments

EMSI · NOVEMBER 17, 2018 · 3 MIN READ

Email remains one of the most common methods of malware delivery. In 2016, about 66 percent of malware was installed via malicious email attachments, according to a Verizon report.

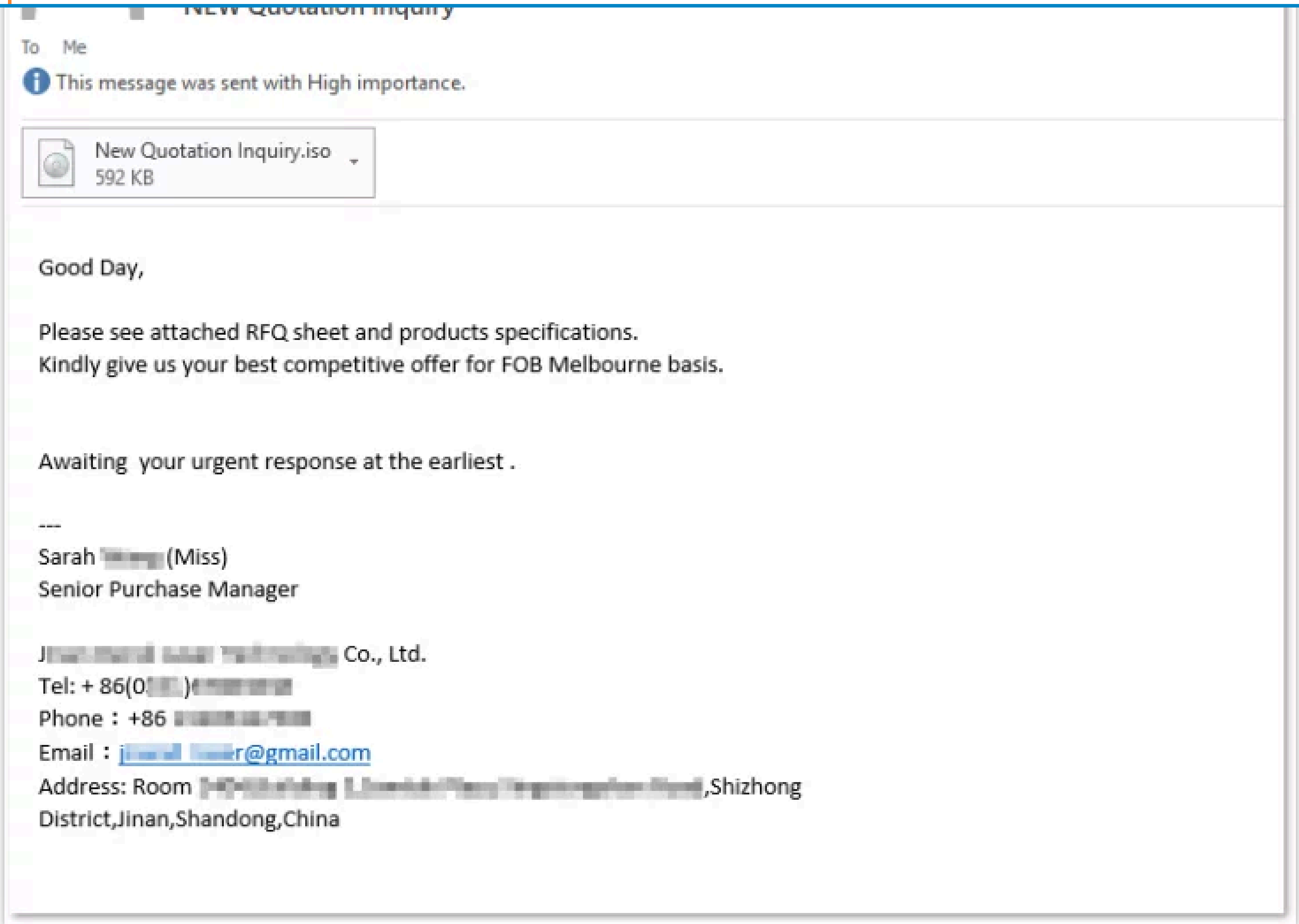
Most malicious email attachments come in the form of widely recognized files such as .EXE, .DOC, .PDF, .ZIP and so on, but recently we've seen a spike in malware concealed in ISO files.

Read on to learn more about what ISO files are, how to spot a dodgy ISO email attachment and what you need to do to keep yourself safe from this type of attack.

Example of an email with a malicious ISO attachment

As with many other phishing attacks, the new breed of ISO malware is distributed as an email attachment. The contents of the email message can vary but tend to feature language that creates a sense of urgency and encourages you to open the attached ISO file.

Here's an example of an email we've seen in the wild:



NEW Quotation Inquiry

To Me

This message was sent with High importance.

New Quotation Inquiry.iso
592 KB

Good Day,

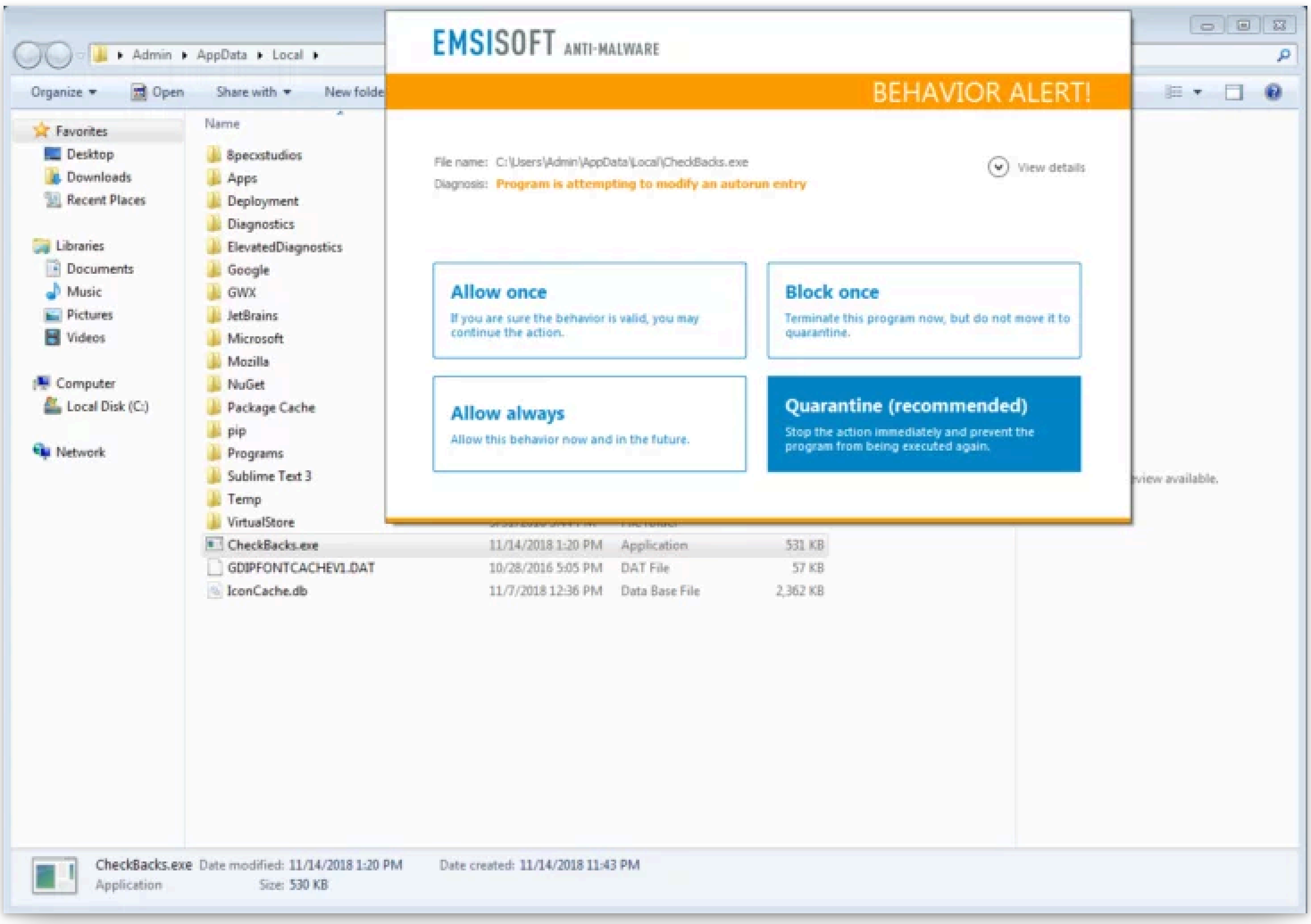
Please see attached RFQ sheet and products specifications.
Kindly give us your best competitive offer for FOB Melbourne basis.

Awaiting your urgent response at the earliest .

Sarah [redacted] (Miss)
Senior Purchase Manager

J[redacted] Co., Ltd.
Tel: + 86(0[redacted])[redacted]
Phone：+86 [redacted]
Email：[redacted]r@gmail.com
Address: Room [redacted],Shizhong
District,Jinan,Shandong,China

In the event that you do open the file, you'll be pleased to know that Emsisoft Anti-Malware will step in to prevent the malware from making any changes to your system. You can see Emsisoft Anti-Malware in action in the screenshot below:



EMSISOFT ANTI-MALWARE

BEHAVIOR ALERT!

File name: C:\Users\Admin\AppData\Local\CheckBacks.exe
Diagnosis: Program is attempting to modify an autorun entry

View details
Allow once
If you are sure the behavior is valid, you may continue the action.
Block once
Terminate this program now, but do not move it to quarantine.
Allow always
Allow this behavior now and in the future.
Quarantine (recommended)
Stop the action immediately and prevent the program from being executed again.
Admin
AppData
Local
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
8pecxstudios
Apps
Deployment
Diagnostics
ElevatedDiagnostics
Google
GWX
JetBrains
Microsoft
Mozilla
NuGet
Package Cache
pip
Programs
Sublime Text 3
Temp
VirtualStore
CheckBacks.exe 11/14/2018 1:20 PM Application 531 KB
GDIPFONTCACHEV1.DAT 10/28/2016 5:05 PM DAT File 57 KB
IconCache.db 11/7/2018 12:36 PM Data Base File 2,362 KB
CheckBacks.exe Date modified: 11/14/2018 1:20 PM Date created: 11/14/2018 11:43 PM
Application Size: 530 KB

What is an ISO file?

An ISO file (sometimes referred to as an ISO image) is an archive file that contains all the program's files in a single file.

Why are ISO files being used?

There are a couple of reasons why ISO files are being used in this attack.

Firstly, the malware authors are probably aware that many email gateway scanners don't scan ISO file attachments properly. This is probably due to the fact that ISOs tend to be hundreds of megabytes in size, making them prohibitively large for efficient and effective scanning. However, ISOs can also be very small and may contain nothing more than a half megabyte malware binary.

Secondly, ISO files are incredibly easy to open these days. In years gone by, you needed third-party software to open an ISO file, but modern versions of Windows (Windows 8 and Windows 10) feature a native ISO mounting tool. Opening an ISO file is now as simple as double-clicking the file. This increases the chances of the target opening the file and infecting their system.

How to protect yourself from ISO malware

The usual rules when it comes to protecting yourself from ISO malware. Be wary of unsolicited emails, avoid clicking links and opening attachments unless you're 100 percent confident that they're safe and always protect yourself with reliable antivirus software.

For more information, please see our guide on identifying and preventing phishing scams.

Have a good (malware-free) day!

Emsi

Emsisoft founder and managing director. In 1998 when I was 16, a so called 'friend' sent me a file via ICQ that unexpectedly opened my CD-ROM drive, which gave me a big scare. It marked the start of my journey to fight trojans and other malware. My story

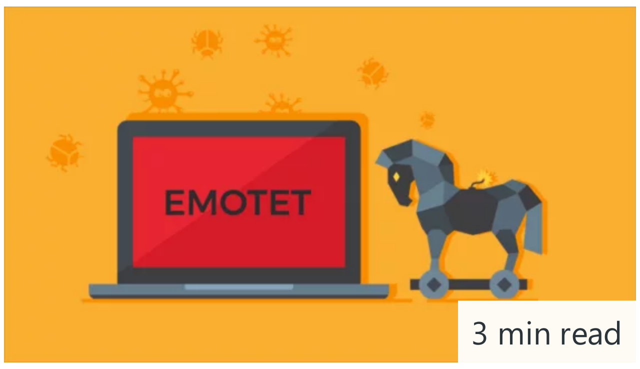
What to read next

4 min read

May 17, 2021 · DECRYPTORS · MALWARE LAB · RANSOMWARE · SECURITY ALERTS

PSA: Threat actors now double encrypting data with multiple ransomware strains

We have recently observed a new trend of threat actors using multiple strains of ransomware to double encrypt data on compromised systems.

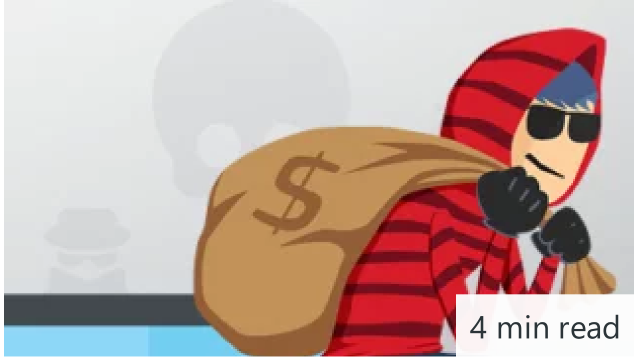


3 min read

Dec 10, 2018 · SECURITY ALERTS

Emotet trojan is back with a vengeance

Emotet is back. The infamous trojan now features an all-new email harvesting module that is helping malware authors create scarily realistic malicious emails.



4 min read

Apr 11, 2017 · MOBILE MALWARE · SECURITY ALERTS

Mobile malware targets Android users

Your mobile phone is the journal of your digital life. Who is reading yours? Emsisoft explores mobile malware and the best ways for you to prevent it.

Newsletter

Malware never sleeps. Be sure to stay up-to-date on emerging threats.

Name... | Email... | Subscribe

□ Emsisoft requires collection and processing of certain personal data to provide the services. Please confirm that you have read and accept the terms of our Privacy Policy.

Emsisoft > Blog > Malware Lab > Security Alerts > Beware: New wave of malware spreads via ISO file email attachments

PRODUCTS

- Emsisoft Business Security
- Emsisoft Enterprise Security
- Emsisoft Remediation Kit
- Emsisoft Anti-Malware Home
- Emsisoft Emergency Kit
- Emsisoft Mobile Security

KEY BENEFITS

- Layered Protection
- Anti-Ransomware
- Centralized Management
- Endpoint Detection & Response
- Threat Hunting
- Ransomware Rollback
- Behavior AI

KNOWLEDGE

- News Blog
- Enterprise Security
- Malware Lab
- Product User Guides
- Video Tutorials

SUPPORT

- Contact Us
- Submit a suspicious file

COMPANY

- About Us
- Our Customers
- Awards & Reviews
- Press Center
- Careers
- Webinars
- Podcast

EMSISOFT - Legal Notice - Terms - Privacy Policy - Cookie Policy - System Status - English

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.