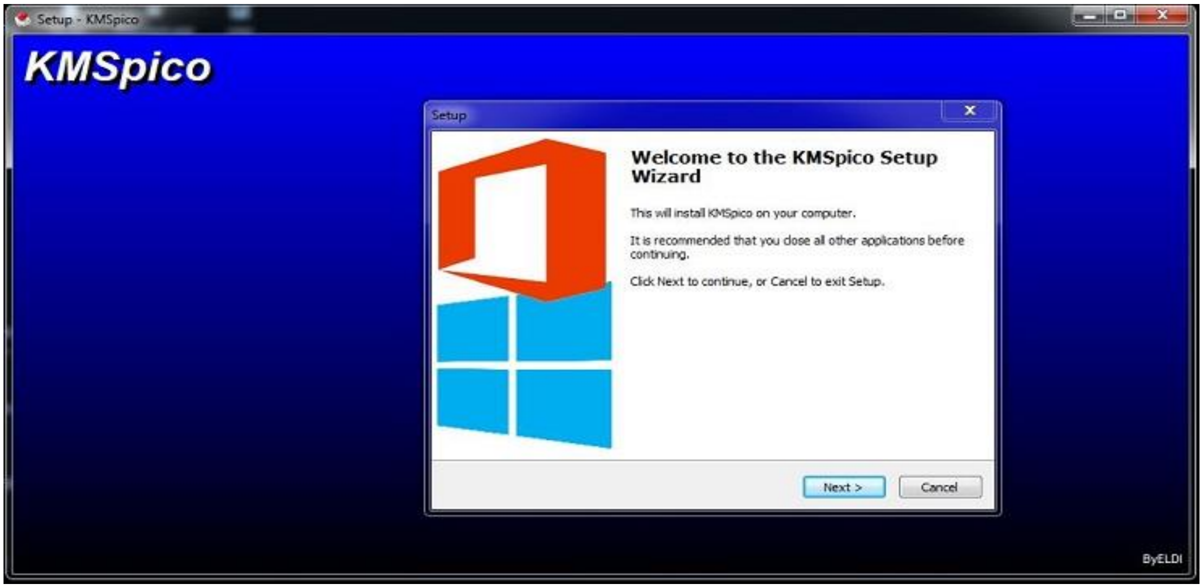
Domino Ransomware Analysis

Domino enters the targeted system when the user tries to install “KMSPico Windows Activation Crack” which seems to be a modified version of KMSPico.



Welcome to the KMSpico Setup Wizard

This will install KMSpico on your computer.

It is recommended that you close all other applications before continuing.

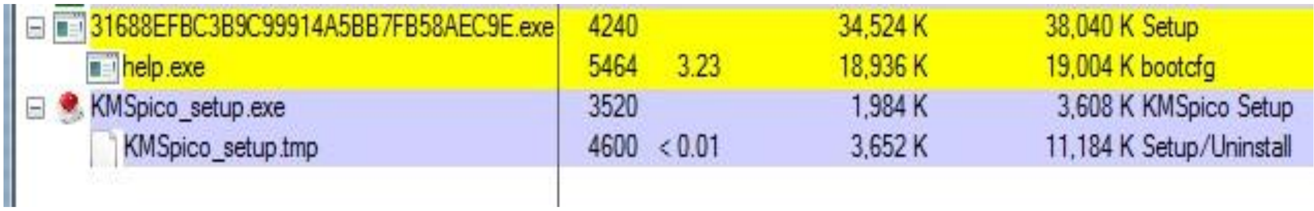
Click Next to continue, or Cancel to exit Setup.

Fig 1. KMSPico Installation

During the installation process, the installer file drops the below components onto the %Temp% location:

- %Temp%\KMSpico_setup.exe
- %Temp%\31688EFBC3B9C99914A5BB7FB58AEC9E.exe
    - %Temp%\help.zip
        - %Temp%\help.exe
        - %Temp%\HelloWorld.exe

These files keep running in memory with the below structure:

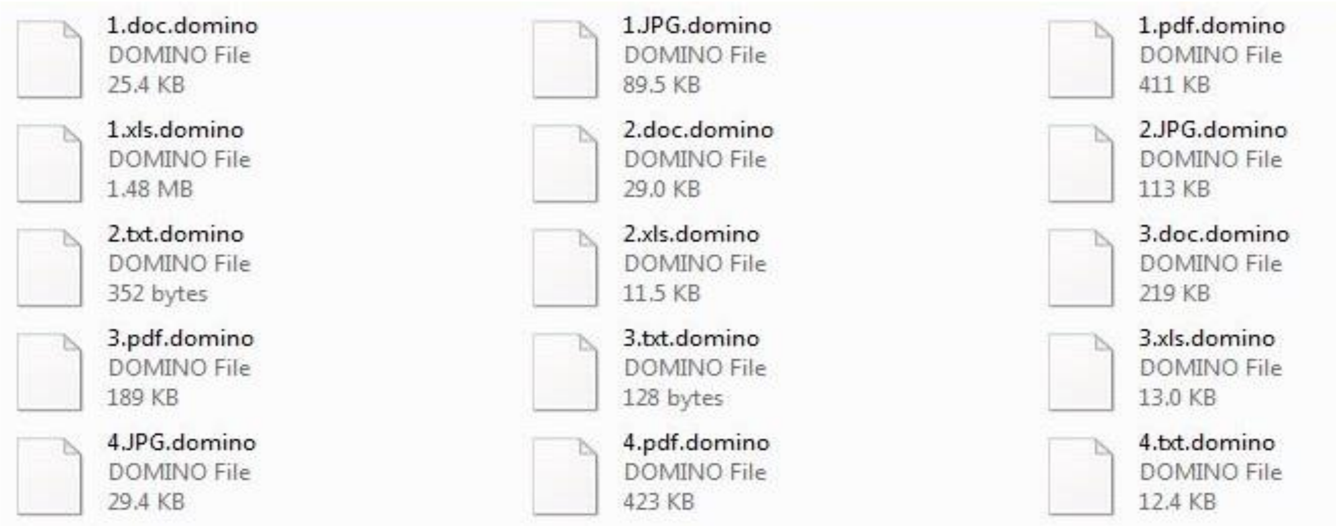


```
31688EFBC3B9C99914A5BB7FB58AEC9E.exe  4240          34,524 K   38,040 K Setup
  help.exe                            5464   3.23   18,936 K   19,004 K bootcfg
KMSpico_setup.exe                     3520           1,984 K    3,608 K KMSpico Setup
  KMSpico_setup.tmp                   4600  < 0.01   3,652 K   11,184 K Setup/Uninstall
```

Fig 2. Dropped components in Execution

Dropped *KMSpico_setup.exe* performs its regular activities. *31688EFBC3B9C99914A5BB7FB58AEC9E.exe* drops *help.zip* which is a password-protected file, containing *HelloWorld.exe* and *help.exe*. This zip file is extracted and executed further by *31688EFBC3B9C99914A5BB7FB58AEC9E.exe*.

help.exe file scans the infected system, encrypts supported files present on it and appends ".domino" to the encrypted files.



1.doc.domino
DOMINO File
25.4 KB

1.JPG.domino
DOMINO File
89.5 KB

1.pdf.domino
DOMINO File
411 KB

1.xls.domino
DOMINO File
1.48 MB

2.doc.domino
DOMINO File
29.0 KB

2.JPG.domino
DOMINO File
113 KB

2.txt.domino
DOMINO File
352 bytes

2.xls.domino
DOMINO File
11.5 KB

3.doc.domino
DOMINO File
219 KB

3.pdf.domino
DOMINO File
189 KB

3.txt.domino
DOMINO File
128 bytes

3.xls.domino
DOMINO File
13.0 KB

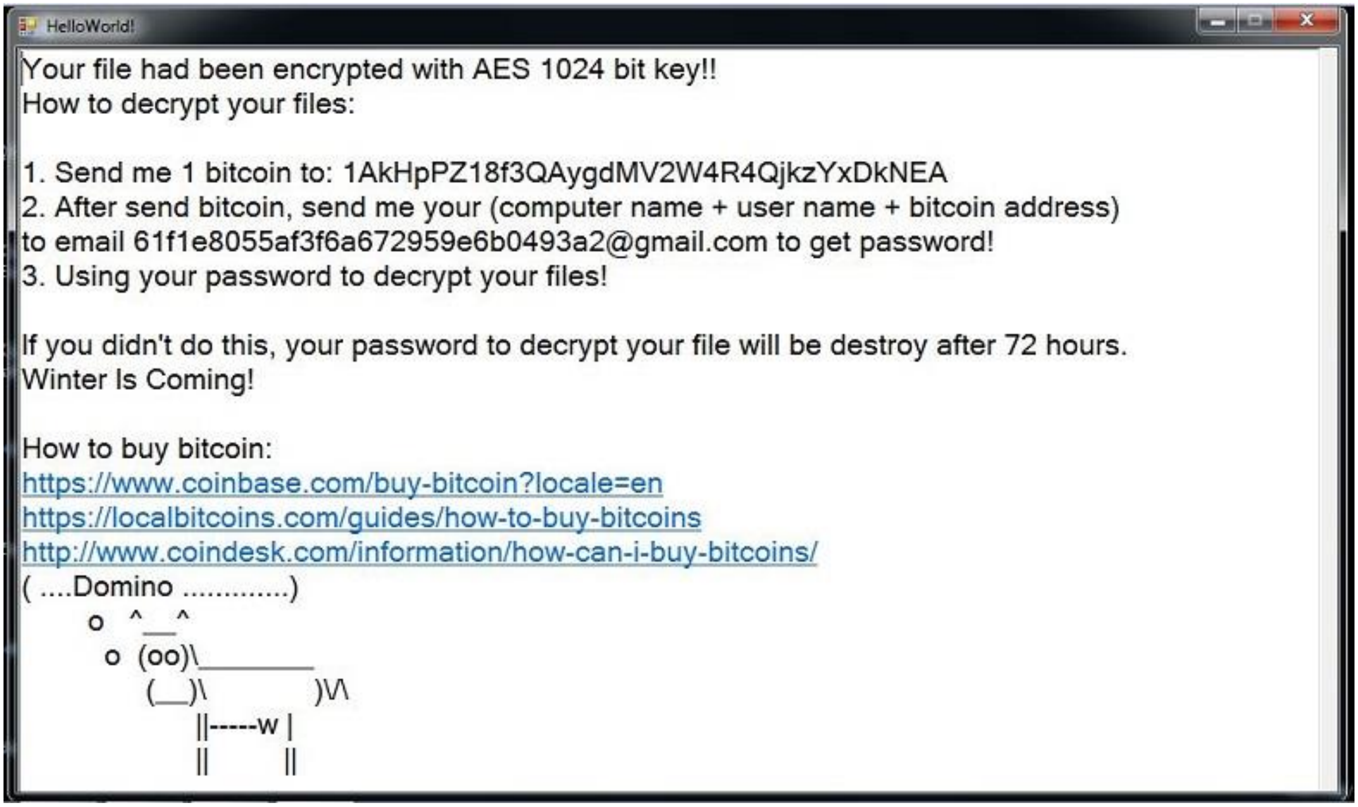
4.JPG.domino
DOMINO File
29.4 KB

4.pdf.domino
DOMINO File
423 KB

4.txt.domino
DOMINO File
12.4 KB

Fig 3. Encrypted Files

When the ransomware completes its encryption activity, *HelloWorld.exe* file is executed and shows the below ransom note, demanding 1 Bitcoin in exchange for a key that can decrypt the victim's encrypted files.



Your file had been encrypted with AES 1024 bit key!!
How to decrypt your files:

1. Send me 1 bitcoin to: 1AkHpPZ18f3QAygdMV2W4R4QjkzYxDkNEA
2. After send bitcoin, send me your (computer name + user name + bitcoin address)
to email 61f1e8055af3f6a672959e6b0493a2@gmail.com to get password!
3. Using your password to decrypt your files!

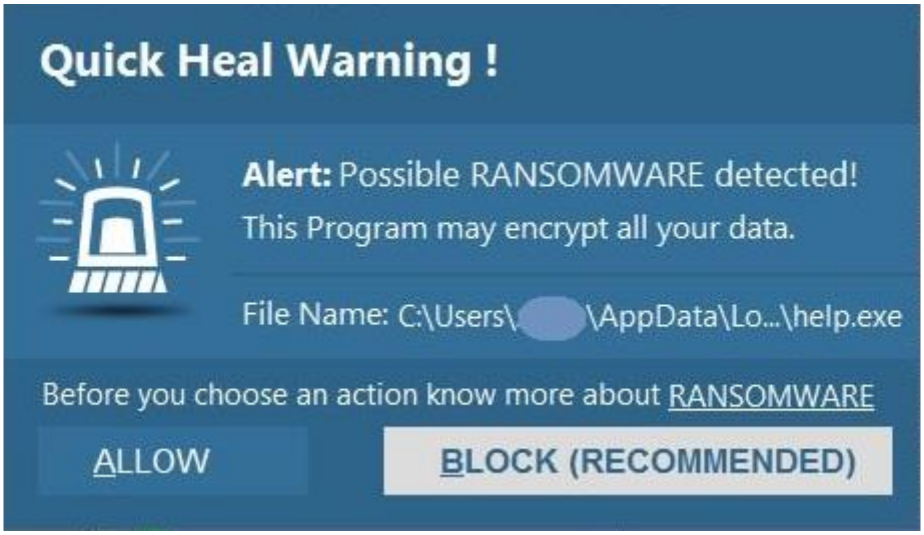
If you didn't do this, your password to decrypt your file will be destroy after 72 hours.
Winter Is Coming!

How to buy bitcoin:
https://www.coinbase.com/buy-bitcoin?locale=en
https://localbitcoins.com/guides/how-to-buy-bitcoins
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

```
( ....Domino .............)
      o   ^__^
        o  (oo)\_________
            (__)\           )\/\
                 ||-----w |
                 ||         ||
```

Fig 4. Ransomware Note

Quick Heal Anti-Ransomware Technology successfully detects the file encryption activity of Domino ransomware.



Quick Heal Warning !

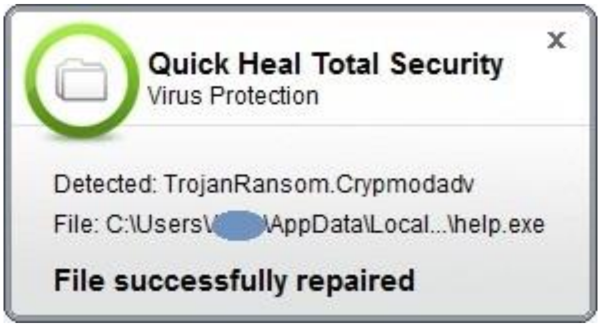
Alert: Possible RANSOMWARE detected!
This Program may encrypt all your data.

File Name: C:\Users\[redacted]\AppData\Lo...\help.exe

Before you choose an action know more about RANSOMWARE

Fig 5. Quick Heal Anti-Ransomware Technology

Quick Heal Virus Protection also successfully detects this malicious ransomware activity as "TrojanRansom.Crypmodadv".



Quick Heal Total Security
Virus Protection

Detected: TrojanRansom.Crypmodadv
File: C:\Users\[redacted]\AppData\Local...\help.exe

File successfully repaired

Fig 5. Quick Heal Virus Protection

Quick Heal detects packed installer of this software as "HackTool.AutoKMS"

As mentioned in the Quick Heal Q2 Threat Report 2016 for Windows, the infection vector of domino ransomware is a good example of a threat which could be caused from the use of Activator software like Activators for Windows, Office, AVs, etc., and Keygens. These software could be exploited by attackers and used to spread malware.